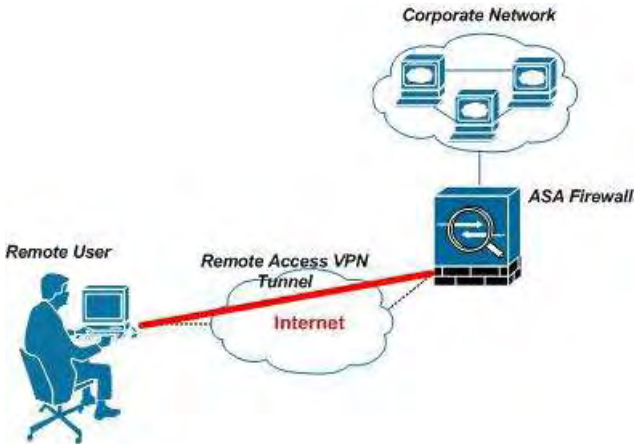
ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Προχωρημένα θέματα ανάλυσης & προσομοίωσης VPN με τη χρήση του εργαλείου Cisco Packet Tracer - Remote Access VPN.



ΑΝΤΩΝΟΠΟΥΛΟΥ ΠΑΝΑΓΙΩΤΑ

ΒΑΣΙΛΕΙΟΥ ΟΛΓΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέποντες
Σταμούλης Γεώργιος, Καθηγητής, Πανεπιστήμιο Θεσσαλίας

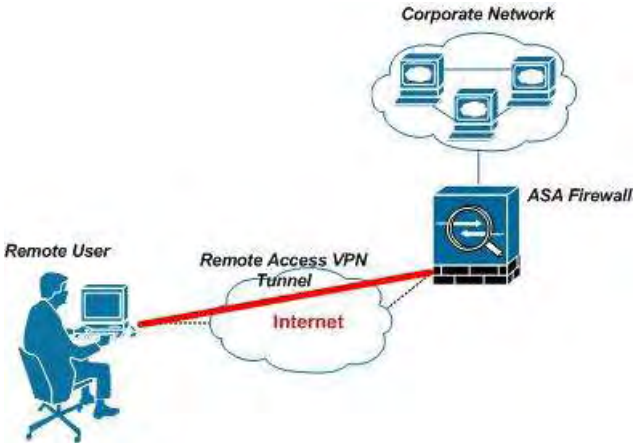
Λαμία, Νοέμβριος 2017

UNIVERCITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Advanced Network Analysis & VPN Simulation using Cisco Packet Tracer - Remote Access VPN.



Antonopoulou Panagiota

Vasileiou Olga

Master thesis

Stamoulis Georgios, University of Thessali

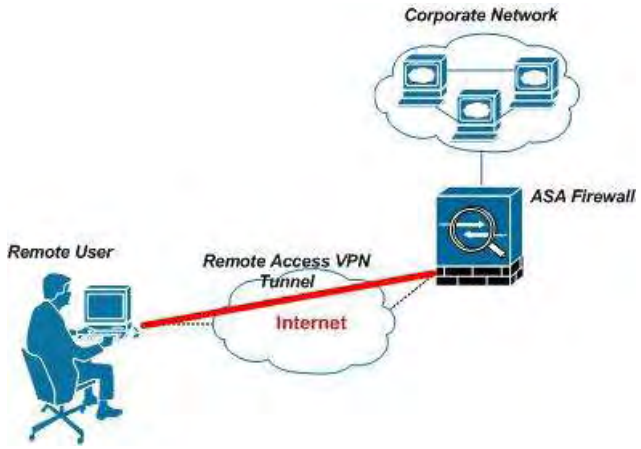
Lamia, November 2017

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΚΑΤΕΥΘΥΝΣΗ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

Προχωρημένα θέματα ανάλυσης & προσομοίωσης VPN με τη χρήση του εργαλείου Cisco Packet Tracer - Remote Access VPN.



ΑΝΤΩΝΟΠΟΥΛΟΥ ΠΑΝΑΓΙΩΤΑ

ΒΑΣΙΛΕΙΟΥ ΟΛΓΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέποντες
Σταμούλης Γεώργιος, Καθηγητής, Πανεπιστήμιο Θεσσαλίας

Λαμία, Νοέμβριος 2017

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Η ΔΗΛΟΥΣΑ

Ημερομηνία

Υπογραφή

Προχωρημένα θέματα ανάλυσης & προσομοίωσης VPN με τη χρήση του εργαλείου Cisco Packet Tracer - Remote Access VPN.

ΑΝΤΩΝΟΠΟΥΛΟΥ ΠΑΝΑΓΙΩΤΑ

ΒΑΣΙΛΕΙΟΥ ΟΛΓΑ

Τριμελής Επιτροπή:

Πρώτος Εξεταστής: (Επιβλέπων) Δρ. Σταμούλης Γεώργιος
Καθηγητής, Τμήμα Πληροφορικής, Πανεπιστήμιο Θεσσαλίας

Δεύτερος Εξεταστής: Δρ. Λουκόπουλος Αθανάσιος
Καθηγητής, Τμήμα Πληροφορικής, Πανεπιστήμιο Θεσσαλίας

Τρίτος Εξεταστής: Δρ. Βαβουγυιός Διονύσιος
Καθηγητής, Τμήμα Πληροφορικής, Πανεπιστήμιο Θεσσαλίας

Επιστημονικός Σύμβουλος:

Κορίνθιος Ιωάννης, Διδάκτωρ Ηλεκτρολόγος Μηχανικός, Ε.Μ.Π.

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε θερμά τον Καθηγητή μας κ. Ιωάννη Κορίνθιο για την ευκαιρία που μας έδωσε να ασχοληθούμε σε βάθος με τη μελέτη ενός προβλήματος με πρακτική εφαρμογή και την προσομοίωση ενός δικτύου. Τον ευχαριστούμε πολύ για την πολύτιμη βοήθειά του σε κάθε στάδιο της εργασίας. Η ανάπτυξη των εικονικών δικτύων τα τελευταία χρόνια είναι μεγάλη και η παρούσα διπλωματική εργασία μας έδωσε την ευκαιρία να μάθουμε πρακτικά τον τρόπο δημιουργίας τους. Η προσομοίωση πραγματοποιήθηκε στο πρόγραμμα μιας από τις μεγαλύτερες εταιρίες στο χώρο των επικοινωνιών και δικτύων, τη CISCO. Επίσης, θα θέλαμε να ευχαριστήσουμε θερμά τον κ. Γεώργιο Σταμούλη, πρόεδρο του τμήματος Πληροφορικής και Υπολογιστικής Βιοϊατρικής, για την πολύτιμη βοήθειά του και τις γνώσεις που μας προσκόμισε καθ' όλη τη διάρκεια φοίτησής μας στο μεταπτυχιακό πρόγραμμα του τμήματος Πληροφορικής του πανεπιστημίου Θεσσαλίας.

Τέλος, επιθυμούμε να αφιερώσουμε την παρούσα διπλωματική εργασία στις οικογένειες μας και τους φίλους μας ως ελάχιστη ανταπόδοση για την ανεκτίμητη υποστήριξη που μας παρείχαν καθ' όλη την ακαδημαϊκή μας πορεία.

ΠΕΡΙΛΗΨΗ

Ο σκοπός της διπλωματικής εργασίας είναι η μελέτη και ανάλυση των τεχνολογιών VPN (Virtual Private Network) και η εφαρμογή της τεχνολογίας VPN μέσω προσομοίωσης διαφορετικών δικτύων VPN με τη χρήση του προγράμματος Cisco Packet Tracer.

Συγκεκριμένα, στα δύο πρώτα κεφάλαια γίνεται αναφορά στις τεχνολογίες των δικτύων επικοινωνίας των απομακρυσμένων υπολογιστών καθώς και η ιστορική εξέλιξη αυτών. Στη συνέχεια αναλύονται ένα προς ένα, όλα τα είδη των VPN, ο τρόπος υλοποίησης τους και οι εφαρμογές τους στον επιχειρησιακό κόσμο.

Στο τρίτο κεφάλαιο αναφέρονται οι τεχνολογίες των VPN ανάλογα με το υλικό που χρησιμοποιείται για την υλοποίηση της λογικής σύνδεσης των απομακρυσμένων υπολογιστών. Επίσης, γίνεται αντιστοίχηση του VPN με τα επίπεδα του πρωτοκόλλου OSI. Ιδιαίτερη έμφαση δίνεται στα ιδιωτικά εικονικά δίκτυα τα οποία βασίζονται στα πρωτόκολλα Multi-Protocol Label Switching (MPLS), Internet Protocol Security (IPSec) και Secure Socket Layer (SSL).

Σημαντικό ρόλο στη σωστή λειτουργία ενός VPN είναι η ασφάλεια μεταφοράς δεδομένων. Στο τέταρτο κεφάλαιο αναλύονται οι αλγόριθμοι κρυπτογράφησης δεδομένων που χρησιμοποιούνται κατά την υλοποίηση της επικοινωνίας μέσω των δικτύων. Επίσης, αναλύονται οι τεχνικές κρυπτογράφησης οι οποίες εφαρμόζονται στα ιδιωτικά εικονικά δίκτυα καθώς και τα είδη των επιθέσεων που αντιμετωπίζουν συνήθως.

Τέλος, το τελευταίο κεφάλαιο επικεντρώνεται στο πρόγραμμα Cisco Packet Tracer και στις δυνατότητες του. Υλοποιούνται δύο προσομοιώσεις ιδιωτικών εικονικών δικτύων. Ένα απλό VPN το οποίο περιλαμβάνει ένα μοναδικό απομακρυσμένο χρήστη, και ένα σύνθετο VPN μιας εταιρείας, στο οποίο συνδέεται ένας απομακρυσμένος χρήστης (Remote User).

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Η αλματώδης πρόοδος της τεχνολογίας χαρακτηρίζει τους τελευταίους αιώνες του ανθρώπινου πολιτισμού, διαμορφώνει τον τρόπο ζωής μας και μας προσφέρει αναρίθμητες και συνεχώς εξελισσόμενες υπηρεσίες. Τα δίκτυα αποτελούν κλειδιά της τεχνολογίας και επιτρέπουν την πρόσβαση χιλιάδων χρηστών σε δικτυακές εφαρμογές που εξυπηρετούν τόσο το εργασιακό όσο και το προσωπικό περιβάλλον μας.

Τα Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPNs) έχουν τις απαρχές τους είκοσι περίπου χρόνια πριν και πρωτοεμφανίστηκαν από μεγάλες εταιρίες, όπως η Microsoft και η Cisco, προκειμένου να βοηθήσουν μεγάλες επιχειρήσεις να μοιράζονται με ασφάλεια υπηρεσίες και πληροφορίες μεταξύ δύο ή περισσότερων σημείων σε διαφορετικές περιοχές. Με το πέρασμα του χρόνου, η αύξηση της εξ΄αποστάσεως εργασίας, αλλά και πιο πρόσφατα η «κινητικότητα» του ανθρώπινου δυναμικού (mobile workforce), έκαναν τα VPNs να αποτελούν αναγκαίο εργαλείο κάθε επιχείρησης, προκειμένου να εξασφαλιστεί ένας ασφαλής τρόπος πρόσβασης σε υπηρεσίες και δεδομένα.

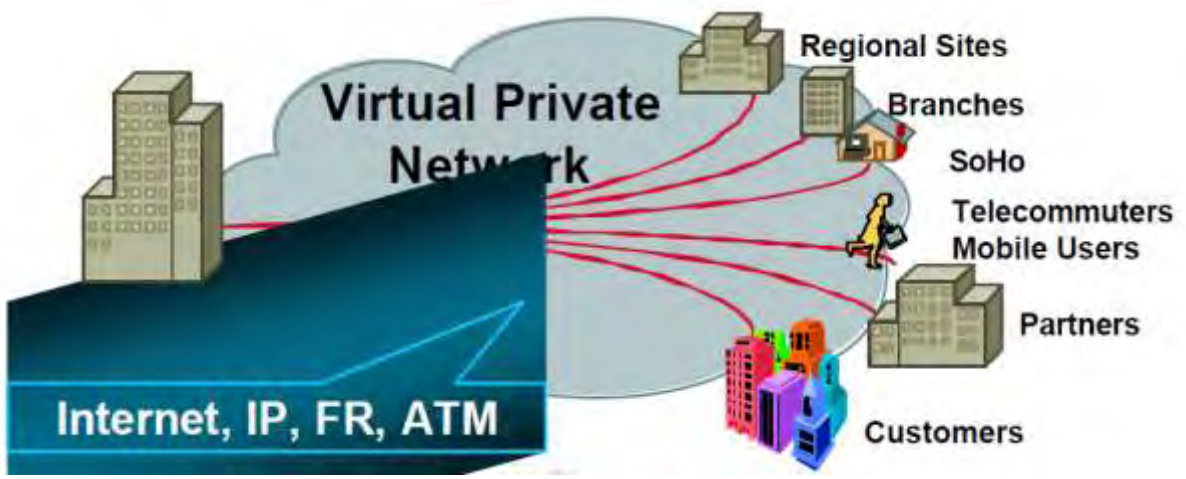
Το πιο βασικό χαρακτηριστικό των δικτύων VPNs είναι ότι παρέχει ασφάλεια σε έναν οργανισμό ή ένα χρήστη. Στις μέρες μας, οι περισσότερες εταιρίες ή οργανισμοί διαθέτουν ένα VPN προκειμένου να διασφαλίσουν τόσο την απομακρυσμένη πρόσβαση των εργαζομένων τους σε εταιρικά περιβάλλοντα, υπηρεσίες και δεδομένα, όσο και την ασφάλεια των δεδομένων αυτών.

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Ορισμοί

Ένα **Virtual Private Network (VPN)** είναι ένα Εικονικό Ιδιωτικό Δίκτυο, το οποίο χρησιμοποιεί ένα πραγματικό Δημόσιο (ή Ιδιωτικό) δίκτυο, όπως είναι το Internet, με σκοπό να οι χρήστες να επικοινωνούν απολαμβάνοντας τις υπηρεσίες ενός Ιδιωτικού Δικτύου. Προσφέρει τη δημιουργία μιας «ασφαλούς» σύνδεσης χτισμένης πάνω σε ένα (στη γενική περίπτωση) μη αξιόπιστο δίκτυο.

Εφόσον πρόκειται για ένα εικονικό δίκτυο, το VPN εγκαθιστά και χρησιμοποιεί εικονικές συνδέσεις δρομολογημένες μέσω του διαδικτύου και άρα συνεισφέρει αποτελεσματικά στην μείωση της απαιτούμενης δικτυακής υποδομής. Ο όρος «Εικονικό» αναφέρεται στο δίκτυο που δημιουργείται έτσι ώστε ένας απομακρυσμένος χρήστης να είναι σε θέση να έχει πρόσβαση στους πόρους ενός ιδιωτικού δικτύου, χωρίς να βρίσκεται φυσικά συνδεδεμένος σε αυτό, αλλά να είναι εικονικά συνδεδεμένος μόνο μέσω του δικτύου VPN.



Εικόνα 1: Ένα VPN δίκτυο επιχείρησης.

Η διασύνδεση των διαφορετικών απομακρυσμένων οντοτήτων (δικτύων ή υπολογιστών) πραγματοποιείται πάνω από μια υποδομή που επιβάλλει την ίδια πολιτική κατά μήκος του εικονικού ιδιωτικού δικτύου, με στόχο να παρέχει το ίδιο επίπεδο ασφαλείας και διαχείρισης και αν είναι δυνατό απόδοσης με ένα πραγματικό ιδιωτικό δίκτυο. Τα εικονικά ιδιωτικά δίκτυα προσφέρουν λοιπόν την λογική διασύνδεση πολλών απομακρυσμένων δικτύων και υπολογιστών, έτσι ώστε όλα μαζί να αποτελούν **ένα ενιαίο δίκτυο ανεξάρτητα από την τοποθεσία τους.**

Ο όρος Virtual Private Network μεταφραζόμενος σε Εικονικό Ιδιωτικό Δίκτυο αναλύεται με μεγαλύτερη λεπτομέρεια σημασιολογικά και πρακτικά παρακάτω.

Το «**Virtual**» μεταφράζεται σαν εικονικό (ιδεατό). Σε αντίθεση με τις μόνιμες συνδέσεις (ασύρματες ή ενσύρματες) μεταξύ των σημείων ενδιαφέροντος, στα VPN η σύνδεση πραγματοποιείται μόνο για το χρονικό διάστημα όπου απαιτείται για την εκτέλεση της εργασίας και κατόπιν διακόπτεται αφήνοντας το δίκτυο και τον εξοπλισμό ελεύθερο για άλλη χρήση. Αυτή η πρακτική έχει προφανή πλεονεκτήματα από πλευράς κόστους και ευελιξίας. Η σύνδεση αποτελεί λογική και όχι φυσική δομή όπως για παράδειγμα στα LANs. Το δίκτυο υφίσταται, μεταβάλλεται, τροποποιείται ανάλογα

με το σημείο και το χρόνο που γίνεται η σύνδεση χρησιμοποιώντας εξωτερικό εξοπλισμό (π.χ. του ISP) και όχι κατά ανάγκη της ίδιας της εταιρίας.

Ο όρος «**Private**» αναφέρεται σε μια προσωπική-ιδιωτική σύνδεση μεταξύ δύο σημείων. Υπονοεί ότι υπάρχει ασφάλεια και προστασία απέναντι σε κάθε είδος υποκλοπής αφού όλα τα δεδομένα θεωρούνται σημαντικά και απόρρητα. Η σύνδεση μεταξύ των δύο σημείων χρησιμοποιεί το υπάρχον δημόσιο δίκτυο μέσω του οποίου ταυτόχρονα μεταφέρονται παράλληλα και άλλα δεδομένα.

Ο όρος «**Network**» αναφέρεται στο κατανεμημένο σύστημα που δημιουργείται από τη διασύνδεση δύο ή περισσότερων τελικών συστημάτων (End Systems ή Hosts) που συνδέονται μεταξύ τους μέσω κάποιου μέσου μετάδοσης (ενσύρματων ή ασύρματων) είτε κατευθείαν είτε μέσω ενδιάμεσων κόμβων (Nodes). Το κατανεμημένο αυτό σύστημα δίνει τη δυνατότητα στους χρήστες (End Users) να ανταλλάσσουν πληροφορίες και δεδομένα.

Ο κυριότερος στόχος ενός VPN είναι να μεταφερθούν πληροφορίες αποτελεσματικά, αποδοτικά και με ασφαλή τρόπο ανεξάρτητα από την απόσταση [1].

1.2 Ιστορική Εξέλιξη

Τα τελευταία χρόνια η χρήση VPN έχει επεκταθεί αρκετά, λόγω των αύξησης των απαιτήσεων των επιχειρήσεων και της προσπάθειας μείωσης του κόστους της υλοποίησης των ιδιωτικών δικτύων. Τα παραδοσιακά ιδιωτικά δίκτυα βασίζονται σε μισθωμένες γραμμές, και παρουσιάζουν μεγάλο κόστος υλοποίησης. Προσπαθώντας να μειώσουν το κόστος αυτό οι επιχειρήσεις στράφηκαν στη χρήση VPN τα οποία χρησιμοποιούν τη δημόσια υποδομή, με τα οφέλη που αυτό συνεπάγεται σε θέματα κόστους.

Τα πρώτα VPN που αναπτύχθηκαν από τους διάφορους οργανισμούς βασίστηκαν κυρίως πάνω σε τεχνολογίες, οι οποίες σήμερα στις περισσότερες περιπτώσεις έχουν ιστορικό χαρακτήρα. Παρακάτω αναφέρουμε επιγραμματικά αυτές τις τεχνολογίες:

- **Μισθωμένες γραμμές** (leased-lines), οι οποίες ενοικιάζονται από τους παρόχους Δικτύου (Network Providers) και είναι αφιερωμένες μόνιμα στον πελάτη,
- **Γραμμές με διεπιλογή** (dial-up lines), οι οποίες χρησιμοποιούνται όταν υπάρχει ανάγκη και ύστερα από την πραγματοποίηση τηλεφωνικής κλήσης προς το δίκτυο του παροχέα, [2]
- **Τεχνολογία X.25 & Τεχνολογία Frame Relay**, οι οποίες είναι τεχνολογίες μεταγωγής πακέτων,
- **Τεχνολογία ISDN** (**Integrated Services Digital Network)**, η οποία επιτρέπει τη μετάδοση πληροφοριών δεδομένων και φωνής σε ψηφιακή μορφή,
- **Τεχνολογία Asynchronous Transfer Mode (ATM)**, η οποία είναι τεχνολογία μεταγωγής πακέτων με χρήση νοητών κυκλωμάτων [3]

Νέες τεχνολογίες έχουν πλέον αναπτυχθεί οι οποίες προσφέρουν πολύ καλή ποιότητα και αξιοπιστία στη σύνδεση, καθώς και μεγάλες ταχύτητες ανταλλαγής δεδομένων. Ενδεικτικά μερικές από τις νέες τεχνολογίες είναι το ADSL, VDSL, Vectoring που παρέχουν ενσύρματη πρόσβαση καθώς και οι τεχνολογίες 3G και 4G που παρέχουν ασύρματη πρόσβαση στους χρήστες.

- **<u>Τεχνολογία ADSL</u>**

Η τεχνολογία ADSL (Asymmetric Digital Subscriber Line) είναι η πιο γνωστή και διαδεδομένη τεχνολογία στις μέρες μας. Η τεχνολογία αυτή έχει σχεδιαστεί έτσι ώστε η αποστολή και η λήψη των δεδομένων να γίνεται σε διαφορετικό εύρος (bandwidth). Συγκεκριμένα, μεγαλύτερο εύρος χρησιμοποιείται στο “downstream”, δηλαδή στην αποστολή δεδομένων προς τον χρήστη, σε σχέση με το “upstream”, δηλαδή στην αποστολή δεδομένων από τον χρήστη. Η ταχύτητα “downstream” κυμαίνεται έως 24 Mbps, ενώ το “upstream” σε πολύ πιο περιορισμένα επίπεδα. Η μεταφορά δεδομένων με την τεχνολογία αυτή είναι διαθέσιμη για αποστάσεις μέχρι λίγα χιλιομετρα μέτρα μέσα από χάλκινο καλώδιο τηλεφωνικής γραμμής**.** [4]

Ενδεικτικά να αναφέρουμε ότι χάρη σ’ αυτή την τεχνολογία οι χρήστες έχουν πλέον τη δυνατότητα να είναι κάθε στιγμή συνδεδεμένοι στο Διαδίκτυο. Παράλληλα, η τεχνολογία ADSL επιτρέπει τη χρήση της τηλεφωνικής γραμμής ταυτόχρονα, δηλαδή ο χρήστης έχει τη δυνατότητα να είναι συνδεδεμένος στο Internet και να κάνει χρήση του τηλεφώνου την ίδια χρονική στιγμή. Τέλος, είναι πολύ αξιόπιστη και προσιτή σε όλους τους χρήστες, καθώς το μηνιαίο τέλος για μια ADSL σύνδεση έχει πλέον μειωθεί σημαντικά.

- **<u>Τεχνολογία VDSL</u>**

Η τεχνολογία VDSL (Very-high-bitrate Digital Subscriber Line service) είναι ο διάδοχος της τεχνολογίας ADSL και εμφανίστηκε στην Ελλάδα το 2008. Η τεχνολογία αυτή προσφέρει γρηγορότερους ρυθμούς μετάδοσης δεδομένων, δηλαδή αναφερόμαστε σε πέντε φορές γρηγορότερη ταχύτητα στο “downstream” και σε δέκα φορές γρηγορότερη ταχύτητα στο “upstream” (30Mbps/2,5Mbps και 50/5Mbps “downstream” και “upstream” αντίστοιχα). Συγκεκριμένα, η τεχνολογία αυτή επιτρέπει τόσο μεγάλες ταχύτητες αξιοποιώντας τη μικρότερη απόσταση στην οποία είναι σχεδιασμένη να λειτουργεί. Αυτό βοηθάει στο να μην έχουμε εξασθένιση του σήματος κατά τη μεταφορά του και να υπάρχει μεγαλύτερη αξιοπιστία στη σύνδεση. [5]

Η τεχνολογία αυτή χρησιμοποιεί για τη μετάδοση των δεδομένων τα χάλκινα τηλεφωνικά καλώδια σε συνδυασμό με καλώδια οπτικών ινών. Το VDSL επιτρέπει την παροχή υπηρεσιών που απαιτούν υψηλό εύρος ζώνης, καθώς μπορεί και **επιτυγχάνει μεγάλες ταχύτητες**. Τέτοιες υπηρεσίες είναι η τηλεόραση υψηλής ανάλυσης, το ψηφιακό βίντεο ή η διασύνδεση απομακρυσμένων εταιρικών δικτύων. [6]

Παρά τις μεγάλες ταχύτητες, ακόμα η τεχνολογία VDSL δεν είναι πολύ διαδεδομένη. Αυτό συμβαίνει διότι έχει κάποια μειονεκτήματα, όπως το **υψηλό κόστος,** το οποίο επιβαρύνεται κάθε χρήστης. Η **μέγιστη απόσταση** στην οποία είναι σχεδιασμένη αυτή η τεχνολογία να λειτουργεί ιδανικά είναι λίγες εκατοντάδες **μέτρα.**

- **<u>Τεχνολογία VDSL Vectoring</u>**

Ο απόγονος της τεχνολογίας VDSL, είναι το VDSL Vectoring. Η τεχνολογία Vectoring δίνει δυνατότητα διπλασιασμού της ταχύτητας του VDSL, φτάνοντας έως τα **100Mbps (downstream)** και τα **40Mbps** (**upstream)**, εξουδετερώνοντας τον «θόρυβο» που δημιουργείται στα καλώδια χαλκού κατά τη μετάδοση του σήματος. Η τεχνολογία αυτή βασίζεται στην αξιοποίηση της ήδη υπάρχουσας

υποδομής (χάλκινα καλώδια και καλώδια οπτικών ινών), χωρίς να επενδύει στη δημιουργία νέου δικτύου με καλώδια οπτικών ινών, επιτυγχάνοντας όμως μεγάλες ταχύτητες και αξιοπιστία. [7]

- **Τεχνολογίες 3G – 4G**

Οι 3G και 4G τεχνολογίες αναφέρονται σε **πρότυπα επικοινωνίας κινητής τηλεφωνίας** που επιτρέπουν την ασύρματη πρόσβαση στο διαδίκτυο, επιτυγχάνοντας **μεγάλες ταχύτητες.**

Το 3G εισήγαγε ουσιαστικά την περιήγηση στο διαδίκτυο, την ανταλλαγή email, το κατέβασμα βίντεο, την ανταλλαγή εικόνων σε smartphone συσκευές. Το 3G επιτυγχάνει αρχικά ταχύτητες από 384 kbps ως **2 Mbps.** Στην συνέχεια με συνεχείς βελτιώσεις του συστήματος η ταχύτητα βελτιώθηκε δραματικά και έφτασε **42 Mbps (downlink) και 11.76 Mbps (uplink).**

Το 4G επιτυγχάνει πολύ μεγαλύτερες ταχύτητες σε σχέση με το 3G, που κυμαίνονται από **100 Mbps έως 1,2 Gbps (downlink) και από 75 Mbps ως 600 Mbps (uplink).** Προκειμένου να πετύχει τις ταχύτητες αυτές, αξιοποιεί περισσότερες από μια συνδέσεις δικτύου στις οποίες μπορεί να έχει πρόσβαση η κινητή συσκευή. Πλέον όλες οι συσκευές κινητής τηλεφωνίας υποστηρίζουν την τεχνολογία αυτή, αλλά και όλοι οι πάροχοι έχουν αναβαθμίσει το δίκτυό τους σε 4G, στην Ελλάδα κυρίως στα μεγάλα αστικά κέντρα και σε περιοχές τουριστικού ενδιαφέροντος. [8]

1.3 Πλεονεκτήματα και Περιορισμοί

Το VPN διαθέτει πολλά πλεονεκτήματα. Αποτελεί μια ιδανική λύση για **ασφαλείς συνδέσεις δικτύου σε μεγάλες αποστάσεις**, μια λύση που εφαρμόζεται σε επιχειρήσεις ή οργανισμούς.

Το προφανές πλεονέκτημα του VPN έγκειται στο ότι, για μια εταιρεία, το **κόστος** του VPN είναι πολύ **χαμηλότερο** από το κόστος των μισθωμένων γραμμών,, των οποίων το μηνιαίο πάγιο είναι εξαιρετικά υψηλό, ιδιαιτέρα για μισθωμένες γραμμές μεγάλων αποστάσεων.

Τα κυριότερο όμως πλεονέκτημα του VPN είναι η ευελιξία του (**Flexibility**), χάρη στην οποία μπορεί να μεταβάλλεται κατά βούληση η διασύνδεση χρηστών στο VPN και να αρκεί απλά και μόνο η σύνδεση με έναν ISP (Internet Service Provider).

Το VPN έχει επεκτασιμότητα (**Scalability**). Δηλαδή, μπορούν όλα τα άτομα που εμπλέκονται στη δράση μιας εταιρείας για παράδειγμα (εργαζόμενοι, πελάτες, προμηθευτές κλπ.), να συνδέονται μεταξύ τους από οποιοδήποτε μέρος του κόσμου. Αυτό συμβαίνει γιατί η σύνδεση στο δίκτυο VPN είναι **εφικτή μέσω του διαδικτύου**, το οποίο προσφέρει απεριόριστη γεωγραφική επέκταση.

Η χρήση του δικτύου VPN **παρέχει μεγάλη ασφάλεια στον χρήστη**, χάρη στα πρωτόκολλα ασφαλείας και tunneling. Αναφέρουμε ως μέσα ασφαλείας – Firewalls, την κρυπτογράφηση δεδομένων και τα πρωτόκολλα ασφαλείας όπως τα IPSec και AAA (Authentication, Authorization, and Accounting). Το πρωτόκολλο IPSec (Internet Protocol Security) διαθέτει καλύτερους αλγορίθμους κρυπτογράφησης και πιο εύχρηστη πιστοποίηση χρηστών. Το πρωτόκολλο AAA παρέχει επιπρόσθετη προστασία, κατά τη σύνδεση των χρηστών σε κάποιο VPN, καθόσον, για να ανοίξει ο χρήστης ένα session, δημιουργείται «αίτηση» η οποία ελέγχει: α) ποιος είναι ο χρήστης (Authentication), β) τι πρόσβαση έχει (Authorization) και γ) τι λειτουργίες πραγματοποιεί (Accounting).

Τέλος, η συγκεντρωτική διαχείριση (**Management**) ενός δικτύου VPN είναι πολύ σημαντική, καθόσον από ένα σημείο είναι δυνατόν να ελέγχονται οι διευθύνσεις IP (addressing), οι πολιτικές πρόσβασης χρηστών, η ασφάλεια και άλλες συναφείς εργασίες.

Η πρόσβαση του χρήστη σε ένα VPN δίκτυο είναι εύκολη, αρκεί να υπάρχει το κατάλληλο λογισμικό δικτύωσης. Η VPN τεχνολογία λειτουργεί το ίδιο καλά είτε μέσω ενσύρματης είτε μέσω ασύρματης σύνδεσης Internet (WI-FI, 3G, 4G).

Βεβαίως, τα VPNs, παρά την δημοτικότητά τους, παρουσιάζουν και **δυνητικά μειονεκτήματα,** όπως κάθε τεχνολογία. Απαιτείται η **εξασφάλιση** επαρκούς **προστασίας** του εικονικού ιδιωτικού δικτύου. Η **αξιοπιστία και η επίδοση** του VPN, που εξαρτάται από το διαδίκτυο, εφόσον αναγκαστικά βασίζεται σε ένα ISP πάροχο και στην ποιότητα των υπηρεσιών του. Ο ακατάλληλος εξοπλισμός, επίσης, μπορεί να προκαλέσει τεχνικά προβλήματα, καθώς επίσης και να αυξήσει το κόστος.

1.4 Εφαρμογές

Ένα VPN μπορεί να προσφέρει λύσεις σε θέματα επικοινωνίας και σε θέματα οργάνωσης, διαχείρισης και κατανομής πληροφοριών και υπηρεσιών.

Μπορεί να έχει εφαρμογή σε επιχειρήσεις με περισσότερα από ένα σημεία παρουσίας, όπως καταστήματα ή γραφεία, τα οποία βρίσκονται μακριά το ένα από το άλλο. Δίνει τη δυνατότητα να συνδέονται μεταξύ τους πελάτες, προμηθευτές, υπάλληλοι, ανεξαρτήτως απόστασης. Επίσης, δίνει τη δυνατότητα σε επαγγελματίες που ταξιδεύουν να χρησιμοποιήσουν το VPN της επιχείρησης, προκειμένου να έχουν πρόσβαση σε όλους τους τοπικούς πόρους δικτύου, σε εκτυπωτές, βάσεις δεδομένων, ιστοσελίδες κλπ. Μπορεί επιπρόσθετα, να έχει εφαρμογή στα εκπαιδευτικά ιδρύματα, για την εξυπηρέτηση φοιτητών και εκπαιδευτικών, με σκοπό την άντληση δεδομένων και τη λήψη υπηρεσιών.

Επιπλέον, ένα VPN δίνει τη δυνατότητα σε ένα χρήστη να αποκρύψει τη δραστηριότητά του από το τοπικό δίκτυο ή ακόμα και από τον ISP στον οποίο είναι συνδεδεμένος. Πιο συγκεκριμένα όταν ένας χρήστης πλοηγείται στο διαδίκτυο, όλες οι ιστοσελίδες που δεν ξεκινούν με το πρόθεμα “https” (Hypertext Transfer Protocol Secure δηλαδή μια ασφαλή δικτυακή σύνδεση http), είναι «εμφανής». με την έννοια ότι δεν υπάρχει κανένα είδος ασφάλειας και κρυπτογράφησης κατά την πλοήγηση. Εάν λοιπόν υπάρχει μια σύνδεση VPN, το μόνο που είναι «ορατό» είναι η σύνδεση αυτή και τίποτα περισσότερο, καθώς πλέον όλες οι πληροφορίες κρυπτογραφούνται.

Τέλος, το δίκτυο VPN μπορεί να έχει εφαρμογή στις ηλεκτρονικές αγορές. Ο χρήστης μπορεί να συνδέεται από μακριά με τον Server του καταστήματος και να στέλνει με ασφάλεια εμπιστευτικές πληροφορίες (username, password, αριθμό πιστωτικής κάρτας), κατά την αγορά προιόντων, καθώς προστατεύει τα δεδομένα με κάποιας μορφής κρυπτογράφηση.

Συμπερασματικά, θα λέγαμε ότι οι VPNs υπηρεσίες κάνουν χρήση διαφόρων τεχνολογιών, καθώς και QoS (Quality of Service) μηχανισμών σε κάποιες περιπτώσεις, για την παροχή λύσεων σε επιχειρήσεις, οργανισμούς ή ιδρύματα, πάνω από το δίκτυο ενός παρόχου, με μειωμένο διαχειριστικό κόστος. [9]

ΚΕΦΑΛΑΙΟ 2: ΜΟΝΤΕΛΛΑ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΕΠΙΚΟΙΝΩΝΙΩΝ

2.1 Μοντέλο αναφοράς OSI

Το πρότυπο OSI (Open Systems Interconnection) καθορίστηκε ως πρότυπο OSI 7498-1 και αναπτύχθηκε ως ένα μοντέλο για το χαρακτηρισμό και την τυποποίηση των λειτουργιών διαστρωματωμένων συστημάτων επικοινωνιών σε όρους επιπέδων ή στρωμάτων (layers).
Βασική αρχή του είναι η αρχή της διαστρωμάτωσης και σύμφωνα με αυτή την αρχή παρόμοιες λειτουργίες ομαδοποιούνται σε λογικά επίπεδα.
Το μοντέλο αναφοράς OSI επηρέασε όχι τόσο τον τρόπο με τον οποίο σχεδιάζουμε όσο τον τρόπο με τον οποίο κατανοούμε τα δίκτυα υπολογιστών. Παρέχει τη βάση αναφοράς για τη διασύνδεση ανοικτών συστημάτων, με σκοπό την υποστήριξη εφαρμογών κατανεμημένης επεξεργασίας. **Ανοικτά συστήματα είναι τα συστήματα τα οποία μπορούν να συνδεθούν καθώς ακολουθούν το μοντέλο αναφοράς OSI και είναι σύμφωνα με αυτό.**
Ο στόχος του OSI και γενικά της προτυποποίησης των πρωτοκόλλων επικοινωνιών είναι τα απομακρυσμένα στοιχεία ενός δικτύου να διαλειτουργούν ανεξάρτητα από το ποιος είναι ο κατασκευαστής τους.
Περί τα τέλη της δεκαετίας του 1980 ο ISO συνιστούσε την εφαρμογή του μοντέλου OSI ως κοινώς αποδεκτού υποδείγματος σχεδιασμού δικτύων. Παρότι δημιουργήθηκαν πρωτόκολλα βασισμένα στο μοντέλο αναφοράς OSI από τον οργανισμό ISO, σε συνεργασία με τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union, ITU), γνωστά ως σειρά πρωτοκόλλων «X» (π.χ. X.25, X.400, X.500 κ.ά.) δεν εφαρμόστηκαν καθώς απέτυχαν εμπορικά.
Εκείνη την εποχή η **στοίβα πρωτοκόλλων TCP/IP, η οποία βασιζόταν σε ελαφρώς διαφορετική διαστρωμάτωση επιπέδων,** ήταν ήδη επί πολύ καιρό σε **χρήση**. Το TCP/IP ήταν θεμελιώδες για το δίκτυο ARPANET και τα άλλα δίκτυα που εξελίχθηκαν στο σημερινό Διαδίκτυο.
Το μοντέλο OSI παραμερίστηκε σταδιακά και σήμερα μόνο ένα υποσύνολό του χρησιμοποιείται ακόμη. Η επικρατούσα αντίληψη είναι ότι οι περισσότερες προδιαγραφές του είναι περίπλοκες και η πλήρης λειτουργικότητά του θα χρειαζόταν μεγάλο χρόνο κατασκευής, αν και συνεχίζουν να υπάρχουν υποστηρικτές του. Έτσι, ιδιαίτερα μετά την εισαγωγή του World Wide Web (WWW) επικρατησε η στοίβα πρωτοκόλλων TCP/IP.
Το μοντέλο αναφοράς OSI έχει επτά επίπεδα. Ένα επίπεδο εξυπηρετεί τόσο το επίπεδο που βρίσκεται πάνω από αυτό, όσο και το επίπεδο που βρίσκεται κάτω από αυτό. Τα τρία χαμηλότερα επίπεδα ασχολούνται με τον έλεγχο της μετάδοσης των μηνυμάτων μέσα στο δίκτυο, ενώ τα τέσσερα ανώτερα επίπεδα παρέχουν την αξιόπιστη μεταβίβαση των δεδομένων μεταξύ των τελικών χρηστών. Έτσι, και τα επτά επίπεδα υλοποιούνται μόνο στους υπολογιστές που λειτουργούν ως τερματικοί σταθμοί. [10]

Τα VPNs έχουν κατά κύριο λόγο, εφαρμογή στο δεύτερο και τρίτο επίπεδο, καθώς είναι τα επίπεδα που συναντιούνται παντού (πρωτόκολλα, δίκτυα, αρχιτεκτονικές κτλ). Σε μερικές περιπτώσεις έχουν εφαρμογή και σε υψηλότερα επίπεδα.

Μοντέλο OSI		
	Επίπεδο	**Λειτουργίες**
Επίπεδα λογισμικού	7.Επίπεδο εφαρμογών (Application Layer)	Παροχή τρόπου στο χρήστη να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου
	6. Επίπεδο παρουσίασης (Presentation Layer)	Τροποποίηση δεδομένων ώστε να είναι κατανοητά από τις εφαρμογές
	5. Επίπεδο συνόδου (Session Layer)	Οργάνωση και συγχρονισμός του διαλόγου
	4. Επίπεδο μεταφοράς (Transport Layer)	Διασφάλιση συνδέσεων, αξιοπιστία
Επίπεδα υλικού	3. Επίπεδο δικτύου (Network Layer)	Δρομολόγηση πακέτων, λογικές διευθύνσεις (IP)
	2. Επίπεδο διασύνδεσης δεδομένων (Data Link Layer)	Αναγνώριση / διόρθωση λαθών, έλεγχος ροής
	1. Φυσικό επίπεδο (Physical Layer)	Ενεργοποίηση υποστήριξη απενεργοποίηση φυσικής διασύνδεσης. Διαμόρφωση / αποδιαμόρφωση δεδομένων

Πίνακας 1: Επίπεδα και λειτουργίες του μοντέλου OSI.

Το Φυσικό Επίπεδο (Physical Layer)

Το φυσικό επίπεδο (physical layer) είναι **το χαμηλότερο επίπεδο του μοντέλου OSI**. Ασχολείται με τη μετάδοση ακατέργαστων bits σε ένα κανάλι επικοινωνίας **(φυσικό μέσο επικοινωνίας)** το οποίο μπορεί να είναι απλή δισύρματη γραμμή, ομοαξονικό καλώδιο, οπτική ίνα ή και ασύρματη ζεύξη. Στο φυσικό επίπεδο **γίνεται μετατροπή των δεδομένων από το επίπεδο 2** (ακολουθία bits) **σε ηλεκτρικά σήματα** και η **μετάδοσή τους μέσω ενός επικοινωνιακού διαύλου (μέσο μετάδοσης).** Τα θέματα σχεδίασης έχουν να κάνουν με τη διασφάλιση ότι, όταν η μία πλευρά στέλνει ένα bit 1, αυτό λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0. Επίσης καθορίζει την διάρκεια κάθε bit, την αρχή και το τέλος της μετάδοσης καθώς και το αν η μετάδοση μπορεί να γίνει προς την μια ή και τις δύο κατευθύνσεις ταυτόχρονα. Τα θέματα σχεδίασης εδώ, στην πλειοψηφία τους ασχολούνται με μηχανικές, ηλεκτρικές και διαδικασίες διασυνδέσεις καθώς και με το **φυσικό μέσο μετάδοσης, το οποίο βρίσκεται κάτω από φυσικό επίπεδο.**

Το φυσικό επίπεδο περιλαμβάνει και τους οδηγούς της κάρτας δικτύου, οι οποίοι λένε στο πρωτόκολλο πώς να πραγματοποιήσει την μετάδοση και την λήψη των δυαδικών ψηφίων. Δικτυακές συσκευές που λειτουργούν στο επίπεδο αυτό είναι **οι κάρτες δικτύου (NICs), τα hubs και οι επαναλήπτες (repeaters).** Οι συσκευές αυτές πραγματοποιούν **λειτουργίες πάνω σε σήματα**. Τα hubs στέλνουν ένα σήμα από μια θύρα σε όλες τις άλλες, οι επαναλήπτες ενισχύουν το σήμα, ώστε

να ταξιδέψει σε μεγαλύτερη απόσταση, ενώ οι κάρτες δικτύου αναλαμβάνουν την σωστή μετάφραση των μεταδιδόμενων σημάτων. [11]

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι (ενδεικτικά):

- Ethernet Physical Layer (IEEE 802.3)
- DSL (Digital Subscriber Line)
- ISDN (Integrated Services Digital Network)
- Bluetooth Physical Layer
- CAN Bus Physical Layer
- Wifi Physical Layer (IEEE 802.3)
- RS232 [12]

Το Επίπεδο Σύνδεσης Δεδομένων (Data Link Layer)

Βασικός σκοπός του επιπέδου αυτού είναι να π**αίρνει τα δεδομένα από το φυσικό επίπεδο και να τα προωθεί στο ανώτερο του επίπεδο, το «επίπεδο δικτύου»**, αφού πρώτα εκτελέσει μερικές ουσιώδεις λειτουργίες όπως είναι η ανίχνευση και διόρθωση σφαλμάτων μετάδοσης και ο έλεγχος ροής των πληροφοριών.

Βεβαίως το επίπεδο αυτό εκτελεί και το αντίστροφο, δηλαδή **δέχεται δεδομένα από το Network Layer (Επίπεδο Δικτύου) και τα αποδίδει στο Physical Layer (Φυσικό Επίπεδο)**. Τα bit που εκπέμπονται ή λαμβάνονται ομαδοποιούνται σε πλαίσια. Τα πλαίσια οργανώνονται σε πεδία που το καθένα έχει διαφορετική αποστολή:

Το **πεδίο διεύθυνσης (address)** παρέχει τις διευθύνσεις του κόμβου αποστολής και του κόμβου παραλαβής.

Το **πεδίο ελέγχου (Flow Control)** δηλώνει το είδος των πλαισίων δεδομένων (αν δηλ. τα πλαίσια είναι πλαίσια δεδομένων, ή πλαίσια διαχείρισης) του καναλιού σύνδεσης.

Το **πεδίο δεδομένων (Data)** περιέχει τα πραγματικά δεδομένα που μεταδίδονται.

Το **πεδίο ελέγχου λαθών**, με βάση αυτό το πεδίο γίνεται ανίχνευση τυχόν λαθών στο πλαίσιο των δεδομένων

Μέρος της επεξεργασίας που γίνεται στα δεδομένα του επιπέδου αυτού είναι και η **προσθήκη των MAC διευθύνσεων του αποστολέα και του παραλήπτη**. Η MAC (Media Access Control) διεύθυνση είναι η διεύθυνση που χαρακτηρίζει μοναδικά μια κάρτα δικτύου και είναι μοναδική. Το επίπεδο 2 χωρίζεται σε δύο υποεπίπεδα, το **υποεπίπεδο ελέγχου λογικού συνδέσμου (Logical Link Control)** και το **υποεπίπεδο ελέγχου προσπέλασης μέσων (MAC).** Δικτυακές συσκευές που λειτουργούν στο επίπεδο αυτό είναι οι **γέφυρες (bridges).** Οι συσκευές αυτές υποστηρίζουν την προώθηση με βάση την MAC διεύθυνση. Η MAC διεύθυνση χρησιμοποιείται για να αποφασίσει η συσκευή αν χρειάζεται να προωθήσει το πλαίσιο από το ένα δίκτυο στο άλλο. Αν η συσκευή έχει πληροφορία για την διεύθυνση αυτή, τότε αποστέλλει το πλαίσιο στον κόμβο που έχει αυτήν την MAC διεύθυνση, αλλιώς προωθεί το πακέτο σε άλλο δίκτυο, στο οποίο πιθανά να βρίσκεται ο κατάλληλος κόμβος. [11]

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι:

- SLIP: Serial Line Internet Protocol
- ARP: Address Resolution Protocol
- PPP: Point-to-Point Protocol
- L2TP: Layer 2 Tunneling Protocol
- PPTP: Point-to-Point Tunneling Protocol
- ISDN: Integrated Services Digital Network [13]
- Ethernet (IEEE 802.3)
- IEEE 802.11 WiFi [12]

Το Επίπεδο Δικτύου (Network Layer)

Βασικές λειτουργίες του επιπέδου είναι η οργάνωσή των δεδομένων σε πακέτα επιπέδου δικτύου, η προώθηση και δρομολόγηση των πακέτων από μια πηγή σε ένα προορισμό, και η διευθυνσιοδότηση των κόμβων και των Hosts.

Καθορίζει το βέλτιστο κάθε φορά μονοπάτι για την μετάδοση της πληροφορίας με βάση την πληροφορία που έχουν για την κατάσταση των συνδέσμων, την διεύθυνση του παραλήπτη, την ταχύτητα του δικτύου, τον αριθμό των ενδιάμεσων κόμβων και μια σειρά άλλων πληροφοριών που διατηρούν. [11]

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι:

- IP: Internet Protocol
- OSPF: Open Shortest Path First
- NAT: Network Address Translation
- ICMP: Internet Control Message Protocol
- BGP: Border Gateway Protocol
- IGMP: Internet Group Management Protocol
- IPSec: Internet Protocol Security
- RIP: Routing Information Protocol
- IPX: Internet Packet Exchange [13]

Το Επίπεδο Μεταφοράς (Transport Layer)

Η βασική λειτουργία του επιπέδου μεταφοράς (transport layer) είναι η **αποδοχή δεδομένων από το ανώτερο επίπεδο ή διάσπαση αυτών σε μικρότερες μονάδες** εάν χρειαστεί, **η μεταφορά τους στο επίπεδο δικτύου** και αναάλογα με την υπηρεσία **η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρά**. Επιπλέον όλα αυτά πρέπει να γίνουν αποδοτικά και με τέτοιο τρόπο ώστε να απομονώνουν το επίπεδο συνόδου από τις αναπόφευκτες αλλαγές στην τεχνολογία του υλικού. Υπό κανονικές συνθήκες, το επίπεδο μεταφοράς δημιουργεί μια ξεχωριστή σύνδεση δικτύου για κάθε σύνδεση μεταφοράς που απαιτείται από το επίπεδο συνόδου. Εάν η σύνδεση μεταφοράς απαιτεί υψηλό ρυθμό εξυπηρέτησης (throughput), το επίπεδο μεταφοράς μπορεί να δημιουργήσει πολλαπλές συνδέσεις δικτύου, μοιράζοντας τα δεδομένα ανάμεσα στις συνδέσεις δικτύου για να βελτιώσει το ρυθμό εξυπηρέτησης.

Από την άλλη πλευρά εάν η δημιουργία ή η συντήρηση μιας σύνδεσης δικτύου είναι ακριβή, το επίπεδο μεταφοράς μπορεί να πολυπλέκει πολλές συνδέσεις μεταφοράς στην ίδια σύνδεση δικτύου για να ελαττώσει το κόστος. Σε όλες τις περιπτώσεις το επίπεδο μεταφοράς χρειάζεται

πάντα για να κάνει την πολυπλεξία διάφανη στο επίπεδο συνόδου. **Το επίπεδο μεταφοράς καθορίζει επίσης τι είδους υπηρεσίες θα παρέχει το επίπεδο συνόδου**. Ο πιο γνωστός τύπος σύνδεσης μεταφοράς είναι ένα ελεύθερο από σφάλματα από σημείο σε σημείο κανάλι (point to point), το οποίο παραδίδει μηνύματα με την σειρά με την οποία έχουν σταλεί [14].

Οι κύριες λειτουργίες του είναι:

- Η Αποκατάσταση και τερματισμός της σύνδεσης σε επίπεδο μεταφοράς
- Η Μετάδοση των δεδομένων σύμφωνα με τον απαιτούμενο από το χρήστη βαθμό αξιοπιστίας (δηλ. με επιβεβαίωση παραλαβής πακέτου ή όχι).
- Ο Καθορισμός και επιλογή από το χρήστη της ποιότητας εξυπηρέτησης της σύνδεσης (όταν αυτό υπάρχει).
- Η Δυνατότητα πολύπλεξης μέσω της ίδιας ζεύξης και ο έλεγχος της ροής.

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι:

- **TCP**: Transmission Control Protocol
- **UDP**: User Datagram Protocol

Το επίπεδο συνόδου (Session Layer)

Το επίπεδο συνόδου (session layer) **επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να εγκαθιστούν συνόδους (sessions) μεταξύ τους**. Μία σύνοδος επιτρέπει μια συνήθη μεταφορά δεδομένων, όπως και το επίπεδο μεταφοράς, αλλά παρέχει και μερικές πρόσθετες υπηρεσίες που είναι χρήσιμες σε πολλές εφαρμογές. Μία σύνοδος μπορεί να χρησιμοποιηθεί για να επιτρέψει τη σύνδεση ενός χρήστη σ' ένα απομακρυσμένο σύστημα καταμερισμού χρόνου (time sharing) ή για να μεταφέρει ένα αρχείο μεταξύ δύο μηχανών. Στο επίπεδο συνόδου γίνεται έλεγχος διαλόγου, δηλαδή ποια συσκευή έχει σειρά για μετάδοση καθώς και συγχρονισμό (παρακολούθηση μεταδόσεων μακράς διάρκειας, π.χ. βίντεο, ώστε να συνεχιστούν από το σημείο που σταμάτησαν σε περίπτωση απότομης διακοπής). [14]

Οι λειτουργίες του επιπέδου αυτού δε χρησιμοποιούνται πάντα και είναι οι εξής:

- Έναρξη και συντήρηση διαλόγου (ή συνόδου) μεταξύ ενός ή περισσοτέρων σταθμών (ταυτόχρονα).
- Διαχείριση και έλεγχος προσπέλασης της κάθε συνόδου.
- Επανορθωτικές διαδικασίες σε επίπεδο διαλόγου (σε περίπτωση προβλήματος). [11]

Το επίπεδο παρουσίασης (Presentation Layer)

Συγκεκριμένα, ενώ όλα τα κατώτερα επίπεδα ενδιαφέρονται μόνο για την αξιόπιστη μετακίνηση bits από το ένα μέρος στο άλλο, **το επίπεδο παρουσίασης καταπιάνεται με το συντακτικό και τη σημασιολογία των πληροφοριών που μεταδίδονται.** Επίσης, το επίπεδο παρουσίασης ενδιαφέρεται και για άλλα θέματα όπως η **αναπαράσταση πληροφοριών**. Για παράδειγμα, η συμπίεση των δεδομένων χρησιμοποιείται για να ελαττώσει τον αριθμό των bits που πρόκειται να μεταδοθούν και συχνά απαιτείται κρυπτογράφηση για να εξασφαλιστεί η μυστικότητα (**privacy**) και η γνησιότητα (**authentication**) της πληροφορίας. Επειδή οι υπολογιστές χρησιμοποιούν διαφορετικά λειτουργικά συστήματα (Windows, Linux, MacOs) είναι απαραίτητο τα δεδομένα να

μετατραπούν σε ένα **κοινό** μορφότυπο (**format**) που να είναι "κατανοητό" και από τους δύο συσκευές που πρόκειται να επικοινωνήσουν. Το επίπεδο παρουσίασης εξασφαλίζει ότι η πληροφορία από το επίπεδο εφαρμογής ενός συστήματος μπορεί να διαβαστεί από το επίπεδο εφαρμογής ενός άλλου συστήματος. **Μετατρέπει τα δεδομένα σε κοινό format και παρέχει υπηρεσίες κρυπτογράφησης, αποκρυπτογράφησης.** Οι λειτουργίες του επιπέδου αυτού δε χρησιμοποιούνται πάντα. [14]

Το επίπεδο εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής (application layer) περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά. Η μεταφορά ενός αρχείου μεταξύ δύο διαφορετικών συστημάτων απαιτεί αντιμετώπιση αυτών και άλλων μη συμβατών καταστάσεων. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών όπως, το ηλεκτρονικό ταχυδρομείο, η εμφάνιση καταλόγων αρχείων και διάφορες άλλες ειδικού και γενικού σκοπού. Είναι **το επίπεδο που είναι πιο κοντά στην εφαρμογή του χρήστη** (π.χ. Firefox, Outlook). Δεν παρέχει υπηρεσίες σε κανένα άλλο επίπεδο του OSI. Πρωτόκολλα αυτού του επιπέδου είναι το HTTP, FTP, Telnet, SMTP. [14]

Οι υπηρεσίες που προσφέρει είναι οι εξής:

- Την εξακρίβωση της ταυτότητας των εφαρμογών που θέλουν να επικοινωνήσουν και την επιβεβαίωση της διαθεσιμότητας τους για συνομιλία.
- Την επιβεβαίωση η τον έλεγχο στο δικαίωμα της συνομιλίας.
- Τον καθορισμό αρμοδιοτήτων.
- Τον καθορισμό των διαδικασιών για τον έλεγχο της ροής των συνόδων και την αξιοπιστία της πληροφορίας. [11]

Μερικά από τα πρωτόκολλα εφαρμογών που συναντούμε στο επίπεδο αυτό είναι:

- HTTP: Hypertext Transfer Protocol
- FTP: File Transfer Protocol
- TFTP: Trivial Transfer Protocol
- TELNET
- SMTP: Simple Mail Transfer Protocol
- SNMP: Simple Network Management Protocol
- IMAP: Internet Message Access Protocol
- POP3: Post Office Protocol version 3
- SET: Secure Electronic Transaction [13]

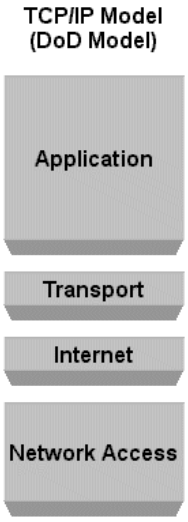
2.2 Στοίβα TCP/IP

Το **TCP/IP (Transmission Control Protocol/Internet Protocol)** είναι παλιότερο μοντέλο από το OSI, ωστόσο είναι αυτό που έχει επικρατήσει σήμερα. Αναπτύχθηκε από το DoD (Department of Defense) των Η.Π.Α. για να υποστηρίξει τη λειτουργία του δικτύου ARPANET, που αποτελεί τον πρόδρομο του σημερινού Internet. Η αρχιτεκτονική αυτή, που ομοιάζει στο μοντέλο αναφοράς OSI, έχει ως βασικό στόχο **τη διατήρηση του δικτύου ακόμη και όταν ένας η περισσότεροι κόμβοι**

καταρρεύσουν. Επίσης, έχει ευελιξία στην αρχιτεκτονική, αφού υποστηρίζει ένα δίκτυο με πολλές εφαρμογές και τη μεταφορά όλων των τύπων πληροφορίας.

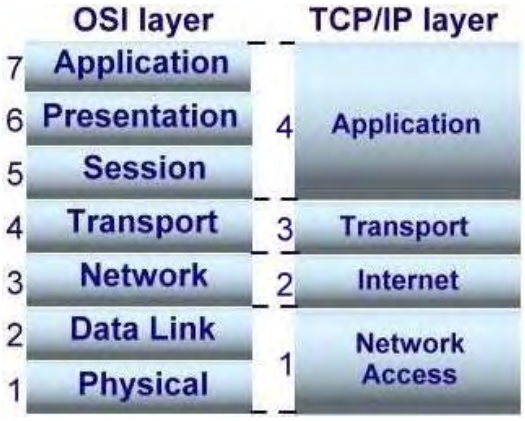
Το μοντέλο TCP/IP αποτελείται από τέσσερα (4) επίπεδα:

- Επίπεδο Διασύνδεσης Δικτύου (Επίπεδο 1)
- Επίπεδο Διαδικτύου (Επίπεδο 2
- Επίπεδο Μεταφοράς (Επίπεδο 3)
- Επίπεδο Εφαρμογών (Επίπεδο 4)



Εικόνα 2: Μοντέλο TCP/IP

Μεταξύ του μοντέλου OSI και TCP/IP υπάρχει αντιστοιχία ως προς τα επίπεδα από τα οποία αποτελούνται. Καθώς το μοντέλο OSI σχεδιάστηκε αργότερα από το TCP/IP οι σχεδιαστές του θέλησαν να εξασφαλίσουν πως το πακέτο πρωτοκόλλων του TCP/IP θα συμπεριλαμβάνονταν στο νέο μοντέλο που σχεδίαζαν καθώς υπήρχαν αρκετά συστήματα τα οποία λειτουργούσαν ήδη με βάση το TCP/IP. Στόχευαν στην ομαλή επικοινωνία με αυτά τα συστήματα. Η αντιστοίχηση των επιπέδων των δύο μοντέλων δίνεται στην εικόνα 3. Το επίπεδο εφαρμογών του TCP/IP αντιστοιχεί στα επίπεδα 5, 6, και 7 του μοντέλου OSI, το επίπεδο μεταφοράς στο επίπεδο 4 του OSI, το επίπεδο διαδικτύου αντιστοιχεί στο επίπεδο 3 του OSI και τέλος το επίπεδο διασύνδεσης δικτύου του TCP/IP αντιστοιχεί στα επίπεδα 1 και 2 του OSI.



Εικόνα 3: Αντιστοίχιση επιπέδων μοντέλου OSI και TCP/IP.

Το Επίπεδο Διασύνδεσης Δικτύου

Το επίπεδο διασύνδεσης δικτύου, είναι **το χαμηλότερο επίπεδο** στην ιεραρχία των επιπέδων του μοντέλου TCP/IP. Αντιστοιχεί στο φυσικό επίπεδο και το επίπεδο συνδέσμου μετάδοσης δεδομένων του μοντέλου του OSI. **Επικοινωνεί απευθείας με το δίκτυο και παρέχει την διασύνδεση μεταξύ της αρχιτεκτονικής του δικτύου (π.χ. Ethernet) και του επιπέδου του διαδικτύου**.

Το Επίπεδο Διαδικτύου

Το επίπεδο διαδικτύου είναι το **βασικότερο επίπεδο του μοντέλου**. Είναι το δεύτερο επίπεδο του μοντέλου και χρησιμοποιεί αρκετά πρωτόκολλα για τη **δρομολόγηση και προώθηση των πακέτων**. Τα πακέτα ταξιδεύουν ανεξάρτητα το ένα από το άλλο προς τον προορισμό τους και πιθανά φτάνουν και με διαφορετική σειρά από αυτή με την οποία έφυγαν από τον αποστολέα τους. **Τα ανώτερα επίπεδα αναλαμβάνουν την ανασυγκρότηση των πακέτων, όποτε απαιτείται**, ώστε η πληροφορία να φτάσει σωστά. Οι λειτουργίες του επιπέδου αυτού είναι αντίστοιχες με τις λειτουργίες του επιπέδου δικτύου του μοντέλου OSI. Στο επίπεδο αυτό συναντούμε αρκετά **πρωτόκολλα**, όπως το ARP και ο ICMP, αλλά σίγουρα το βασικότερο και πλέον γνωστό είναι το **IP**. **Το IP είναι ένα πρωτόκολλο μεταγωγής πακέτων που είναι υπεύθυνο για τη διευθυνσιοδότηση και την προώθηση.** Βασικός στόχος του είναι να προωθεί τα πακέτα στον προορισμό τους, όσο το δυνατόν πιο γρήγορα και αποφεύγοντας τις συμφορήσεις του δικτύου.

Το Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς είναι υ**πεύθυνο για την εγκαθίδρυση και διατήρηση της επικοινωνίας μεταξύ δύο υπολογιστών**. Κύρια λειτουργία του είναι να αναλαμβάνει τον έλεγχο ροής και την τοποθέτηση των πακέτων στη σωστή σειρά, ώστε η πληροφορία να λαμβάνεται τελικά ακέραια και ορθή. Χειρίζεται επίσης και τις αναμεταδόσεις των πακέτων.

Στο επίπεδο αυτό έχουν οριστεί δύο πρωτόκολλα μεταφοράς από άκρο σε άκρο:

- Το πρώτο είναι το **TCP** (Πρωτόκολλα Ελέγχου Μετάδοσης) και
- Το πρωτόκολλο **UDP** (Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη). [11]

Το TCP είναι ένα **αξιόπιστο συνδεσμοστρεφές πρωτόκολλο** υπεύθυνο για την αξιόπιστη μετάδοση δεδομένων από έναν κόμβο σε κάποιον άλλο. Για να εγκαθιδρύσει μια αξιόπιστη σύνδεση το TCP χρησιμοποιεί την γνωστή ως «τριμερή χειραψία» **(three-way handshake) με την οποία καθορίζεται ο αριθμός θύρας που θα χρησιμοποιηθεί για την επικοινωνία** καθώς και οι αρχικοί ακολουθιακοί αριθμοί για την μεταφορά των δεδομένων. Το TCP χειρίζεται τα δεδομένα σαν μια ακολουθία (stream) από bytes.

Το User Datagram Protocol (UDP) είναι ένα **αναξιόπιστο ασυνδεσμικό πρωτόκολλο** το οποίο χρησιμοποιείται σε περιπτώσεις όπου **δεν απαιτείται** παράδοση των πακέτων με τη σωστή σειρά ή ο έλεγχος ροής που πραγματοποιείται με την χρήση του TCP. Ο οποιοσδήποτε έλεγχος γίνεται από την εφαρμογή που κάνει χρήση του συγκεκριμένου πρωτοκόλλου. Χρησιμοποιείται επίσης ευρέως σε περιπτώσεις όπου απαιτείται ταχύτατη παράδοση των πακέτων και δεν είναι τόσο κρίσιμη η

αξιόπιστη μετάδοσή τους. Τέτοιες περιπτώσεις είναι η μετάδοση βίντεο και ήχου. Και το UDP κάνει χρήση θυρών, ωστόσο αυτές διαφέρουν από τις αντίστοιχες του TCP και επομένως τα δύο πρωτόκολλα μπορούν να χρησιμοποιούν τον ίδιο αριθμό θυρών χωρίς διενέξεις. [15]

Το Επίπεδο Εφαρμογών

Το επίπεδο εφαρμογών είναι το **υψηλότερο επίπεδο του μοντέλου**. Αυτό περιέχει όλα τα πρωτόκολλα ανώτερου επιπέδου. Μερικά αυτά είναι:

- FTP: File Transfer Protocol
- TELNET
- DNS: Domain Name System
- HTTP: Hypertext Transfer Protocol
- SMTP: Simple Mail Transfer Protocol
- NNTP: Network News Transport Protocol [16]

2.3 Περιγραφή Βασικών Πρωτοκόλλων

Μερικά σημαντικά πρωτόκολλα περιγράφονται στην ενότητα αυτή.

2.3.1 Πρωτόκολλο IP

Το **IP (Internet Protocol)** είναι είναι το κύριο **πρωτόκολλο του επιπέδου δικτύου** στο **μοντέλο TCP/IP**. Κατ' αντιστοιχία είναι ένα **πρωτόκολλο του τρίτου επιπέδου του μοντέλου OSI**, του επιπέδου δικτύου. **Περιλαμβάνει πληροφορίες** σχετικά με την **διεύθυνση των δεδομένων** καθώς και ορισμένες πληροφορίες ελέγχου ώστε τα πακέτα να δρομολογούνται σε ένα δίκτυο. Είναι εξίσου **κατάλληλο τόσο για τοπικά δίκτυα (LAN) όσο και για WAN επικοινωνίες**. [17]
Το **στρώμα δικτύου** ασχολείται με τη μεταφορά πληροφορίας από τον υπολογιστή **αποστολέα** (Host A) στον απομακρυσμένο υπολογιστή δέκτη (Host B). Στην πλευρά αποστολής ενθυλακώνει τα τμήματα (Segments) που παραλαμβάνει από το επίπεδο μεταφοράς σε πακέτα (packets/datagrams). Στην **πλευρά του δέκτη**, παραδίδει τα τμήματα στο **στρώμα μεταφοράς**. Σε κάθε υπολογιστή (Host) και δρομολογητή (Router) πρέπει να υπάρχουν τα πρωτόκολλα στρώματος δικτύου. Οι δρομολογητές είναι οι ενδιάμεσοι δικτυακοί κόμβοι μεταξύ του αποστολέα (Host A) και του παραλήπτη (Host B), που εξετάζουν τα πεδία της κεφαλίδας όλων των IP πακέτων που περνούν από αυτούς (και όχι την πληροφορία χρήστη και φροντίζουν για την προώθηση/δρομολόγηση των πακέτων . [18]

Το IP πρωτόκολλο έχει δύο κύριες αρμοδιότητες:

- Τη βέλτιστη δυνατή μετάδοση των δεδομένων σε πακέτα (datagrams) μέσω ενός δικτύου χωρίς σύνδεση,
- τον κατακερματισμό και την επανα-συναρμολόγηση των πακέτων.

Η **Διευθυνσιοδότηση** είναι αναπόσπαστο μέρος της διαδικασίας της δρομολόγησης πακέτων δεδομένων IP μέσω του δικτύου. Κάθε διεύθυνση IP αποτελείται από συγκεκριμένα στοιχεία και

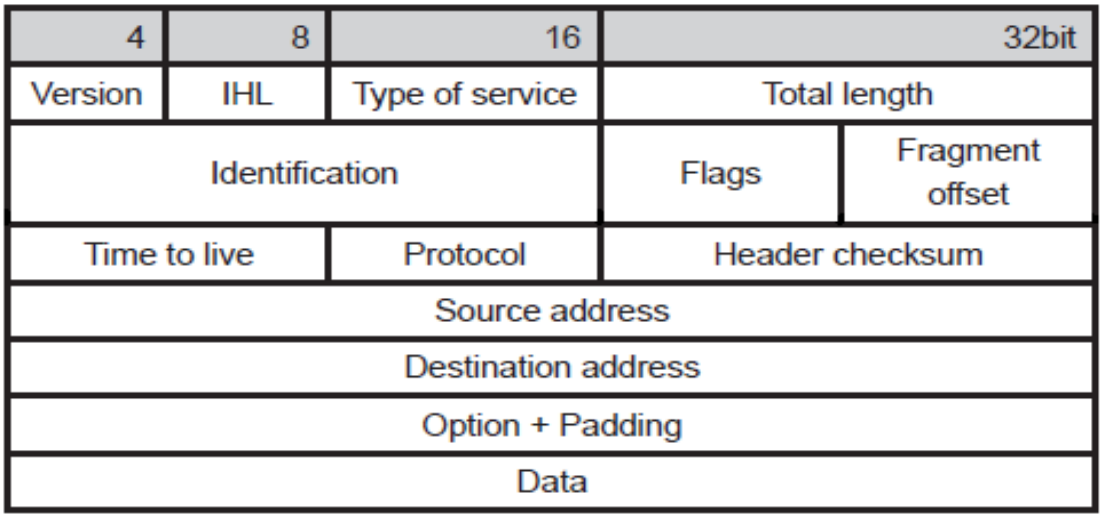
ακολουθεί μια βασική μορφή. Αυτές οι διευθύνσεις IP μπορούν να υποδιαιρεθούν και να χρησιμοποιηθούν για τη δημιουργία διευθύνσεων για υπο-δίκτυα. Κάθε υπολογιστής (host) σε ένα TCP/IP δίκτυο διαθέτει μία μοναδική **32-bit λογική διεύθυνση που χωρίζεται σε δύο κύρια μέρη**:

- τον αριθμό του δικτύου
- τον αριθμό του υπολογιστή (host).

Ο **αριθμός του δικτύου προσδιορίζει ένα δίκτυο και πρέπει να χορηγείται από το Internet Network Information Center (Inter NIC)** εάν το δίκτυο είναι μέρος του Διαδικτύου. Μια υπηρεσία παροχής Internet (ISP) μπορεί να αποκτήσει ένα μπλοκ διευθύνσεων δικτύου από το Inter NIC και μπορεί να αποδώσει τις διευθύνσεις, όπου απαιτείται. Ο **αριθμός του υπολογιστή προσδιορίζει ένα συγκεκριμένο υπολογιστή** σε ένα δίκτυο και έχει εκχωρηθεί από τον διαχειριστή του **τοπικού δικτύου.**

Όταν στέλνετε ή λαμβάνετε δεδομένα (για παράδειγμα, ένα email ή μια σελίδα Web), το μήνυμα χωρίζεται σε μικρά κομμάτια που ονομάζονται **πακέτα**. Κάθε ένα από αυτά τα πακέτα περιέχει τόσο τη **διεύθυνση του αποστολέα στο διαδίκτυο, όσο και τη διεύθυνση του παραλήπτη**. Επειδή ένα μήνυμα είναι χωρισμένο σε ένα αριθμό πακέτων, κάθε πακέτο μπορεί να αποστέλλεται από μια διαφορετική διαδρομή μέσω του Internet. Τα πακέτα μπορούν να φτάνουν σε μια διαφορετική σειρά από τη σειρά που στάλθηκαν. Αυτό αντικατοπτρίζει το γεγονός ότι το IP είναι ένα πρωτόκολλο απλά σχεδιασμένο με στόχο την αποδοτικότητα και δεν υποστηρίζει μηχανισμούς ελέγχου της αξιοπιστίας και διατήρησης της παρεχόμενης ποιότητας υπηρεσίας.

Το πρωτόκολλο ελέγχου μετάδοσης **(Transmission Control Protocol - TCP) ασχολείται με την τοποθέτηση των πακέτων στη σωστή σειρά προσφέροντας έτσι ένα αξιόπιστο μηχανισμό μεταφοράς των πακέττων από άκρη-σε-άκρη .** Όλα τα άλλα πρωτόκολλα εντός της σουίτας TCP/IP, εκτός από το Address Resolution Protocol (ARP) και το Reverse Address Resolution Protocol (RARP), χρησιμοποιούν το IP για να δρομολογήσουν τα πλαίσια από υπολογιστή σε υπολογιστή. Ένα **IP πακέτο** αποτελείται από το **τμήμα της επικεφαλίδας** και το **τμήμα δεδομένων**. Υπάρχουν δύο βασικές εκδόσεις IP, το **IPv4** και το **IPv6**. Η δομή της επικεφαλίδας του IPv4 πρωτοκόλλου φαίνεται στην εικόνα 4. [17]



Εικόνα 4: Δομή πρωτοκόλλου IPv4.

Η επικεφαλίδα στο IPv4 αποτελείται από 14 πεδία, από τα οποία τα 13 είναι απαραίτητα. Παρακάτω αναλύουμε κάθε πεδίο του IPv4 πρωτοκόλλου ξεχωριστά.

- ***Version***

Αποτελείται από 4-bit και υποδεικνύει την έκδοση του IP η οποία χρησιμοποιείται και σήμερα.

- ***IP Header Length (IHL)***

Δίνει το μήκος της επικεφαλίδας σε λέξεις των 32 bits. Επειδή η επικεφαλίδα του IPv4 μπορεί να περιέχει μεταβλητό αριθμό επιλογών, αυτό το πεδίο παρέχει το μήκος της επικεφαλίδας. Επισημαίνει την αρχή των δεδομένων. Η ελάχιστη τιμή για μια σωστή κεφαλίδα είναι 5 που σημαίνει ότι το μήκος είναι 5×32 = 160 bits = 20 bytes. Επειδή το πεδίο είναι 4 bit, το μέγιστο μήκος είναι 2^4-1=15 λέξεις (15×32 bits) ή 480 bits = 60 bytes.

- ***Type-of-Service***

Αναφέρεται στην ποιότητα των παρεχόμενων υπηρεσιών καθορίζοντας πως ένα πρωτόκολλο του ανώτερου στρώματος διαχειρίζεται το πακέτο ως προς το επίπεδο σημασίας. Το πεδίο αποτελείται από 8 bits τα οποία χρησιμοποιούνται για να δείξουν την προτεραιότητα, την καθυστέρηση, την απόδοση και την αξιοπιστία.

- ***Total length***

Αναφέρεται στο συνολικό μήκος, σε bytes, του κομματιού (fragment) συμπεριλαμβανομένων της επικεφαλίδας και των δεδομένων του πακέτου IP. Το ελάχιστο μήκος του πακέτου είναι 20 bytes (20 bytes επικεφαλίδα +0 bytes δεδομένα) και το μέγιστο μήκος είναι 216-1=65535 bytes, καθότι το μήκος του πεδίου είναι 16 bits. Διάφορες συσκευές και μερικές φορές τα υπο-δίκτυα μπορεί να επιβάλλουν περιορισμούς στο μέγεθος των αυτοδύναμων πακέτων, τα οποία σ' αυτήν την περίπτωση πρέπει να σπάσουν σε μικρότερα κομμάτια. Στο IPv4 η διάσπαση των πακέτων μπορεί να γίνει στους σταθμούς εργασίας ή στους δρομολογητές. [17]

- ***Identification***

Είναι ένα πεδίο ταυτότητας των 16 bits, περιέχει έναν ακέραιο αριθμό ο οποίος προσδιορίζει το τρέχον πακέτο. Αυτό το πεδίο έχει ανατεθεί από τον αποστολέα με σκοπό να βοηθήσει τον δέκτη για να συγκεντρώσει όλα τα τμήματα της αρχικής κατακερματισμένης πληροφορίας.

- ***Flags***

Είναι ένα πεδίο των 3-bits και χρησιμεύει να ελέγχει ή να προσδιορίζει τα κομμάτια του πακέτου. Το bit (χαμηλής τάξης) καθορίζει εάν το πακέτο μπορεί να κατακερματιστεί (DF=Don't Fragment). Το μεσαίο bit καθορίζει εάν το πακέτο είναι το τελευταίο κομμάτι σε μια σειρά κατακερματισμένων πακέτων (MF=More Fragments). Το τρίτο bit (υψηλής τάξης) δεν χρησιμοποιείται.

- ***Fragment Offset***

Αποτελείται από 13-bits και είναι ένα πεδίο το οποίο υποδεικνύει τη θέση του κατακερματισμένου πακέτου μέσα στο αρχικό σύνολο δεδομένων. Το πεδίο επιτρέπει στην πορεία της διαδικασίας αποστολής να ανακατασκευαστεί σωστά η αρχική πληροφορία από τα πακέτα.

- ***Time-to-Live***

Αποτελείται από 8 bits και είναι ένας μετρητής που μειώνεται σταδιακά σε κάθε δρομολογητή κατά ένα. Όταν φτάσει στο μηδέν τότε το πακέτο απορρίπτεται. Σκοπός του πεδίου είναι να απορρίψει πακέτα τα οποία ταξιδεύουν άσκοπα στο δίκτυο. Όταν ένα πακέτο απορριφθεί τότε στέλνεται ένα μήνυμα πίσω στον αποστολέα [19].

- ***Protocol***

Το πεδίο protocol αποτελείται από 8 bits και καθορίζει ποιο πρωτόκολλο του ανωτέρου επιπέδου, δηλαδή του επιπέδου μεταφοράς αναλαμβάνει τα εισερχόμενα πακέτα μετά την ολοκλήρωση της επεξεργασία IP.

- ***Header Checksum***

Αποτελείται από 16-bits και είναι ένα άθροισμα με το οποίο γίνεται έλεγχος της επικεφαλίδας, για τον εντοπισμό σφαλμάτων. Μόλις ένα **πακέτο** φτάσει σε έναν δρομολογητή, ο δρομολογητής υπολογίζει το άθροισμα ελέγχου της επικεφαλίδας και το **συγκρίνει με το πεδίο header checksum της επικεφαλίδας**. Εάν δεν ταιριάζουν, τότε ο δρομολογητής απορρίπτει το πακέτο. Όταν ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής μειώνει το πεδίο χρόνου ζωής (Time To Live – TTL). Συνεπώς ο δρομολογητής πρέπει να υπολογίσει το νέο άθροισμα ελέγχου.

- ***Source Address***

Είναι το πεδίο που καθορίζει την διεύθυνση IPv4 του αποστολέα των πακέτων. Αποτελείται από 32 bits.

- ***Destination Address***

Είναι το πεδίο που καθορίζει την διεύθυνση IPv4 του προορισμού των πακέτων. Αποτελείται από 32 bits [17]

- ***Options***

Αυτό το πεδίο αντιπροσωπεύει μια λίστα επιλογών για ένα συγκεκριμένο datagram IP. Είναι ένα προαιρετικό πεδίο. Βασικές επιλογές είναι η χρονοσφραγίδα, η καταγραφή διαδρομής που ακολουθείται, ο καθορισμός λίστας δρομολογητών που θα επισκεφτεί κ.α. [18]

- ***Data***

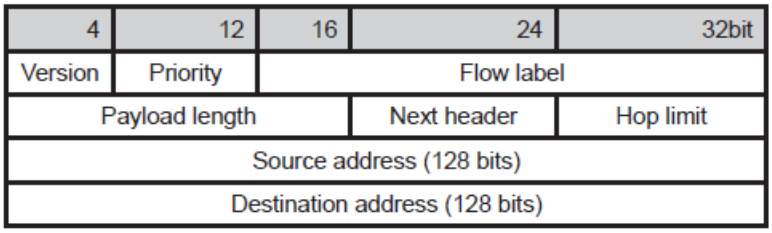
Το πεδίο αυτό περιλαμβάνει τα δεδομένα από το επίπεδο του πρωτοκόλλου (protocol layer) το οποίο συνεργάζεται με το επίπεδο IP (IP layer) για τη μεταφορά των δεδομένων. Γενικά αυτό το επίπεδο περιλαμβάνει την επικεφαλίδα και τα δεδομένα από το επίπεδο μεταφοράς (transport layer). Αξίζει να σημειωθεί ότι κάθε επίπεδο στο TCP/IP έχει τη δική του επικεφαλίδα στην αρχή των δεδομένων. Η επικεφαλίδα (header) περιλαμβάνει πληροφορίες για την προέλευση των δεδομένων όταν αυτά προέρχονται από κάποιο άλλο επίπεδο. Σε περίπτωση που στέλνει δεδομένα σε άλλα επίπεδα, το πρωτόκολλο δημιουργεί τη δική του επικεφαλίδα (header). [19]

Το **IPv6** είναι η νέα έκδοση του πρωτοκόλλου Internet (IP) και βασίζεται στην έκδοση IPv4. Είναι ένα πρωτόκολλο του επιπέδου δικτύου (Layer 3) το οποίο περιέχει πληροφορίες διευθυνσιοδότησης και μερικές πληροφορίες ελέγχου της δρομολόγησης των πακέτων στο δίκτυο. Το πρωτόκολλο IPv6 ονομάζεται νέας γενιάς IP ή IPng και δημιουργήθηκε για να επιλύση το πρόβλημα εξάντλησης διευθύνσεων του IPv4 .

Ενώ το IPv4 χρησιμοποιεί διευθύνσεις 32 bits το IPv6 αυξάνει το μέγεθος σε 128 bits, υποστηρίζοντας περισσότερα επίπεδα διευθυνσιοδότησης, σε ένα μεγαλύτερο αριθμό κόμβων και απλούστερη αυτόματη διαμόρφωση των διευθύνσεων. Οι διευθύνσεις στο IPv6 εκφράζονται σε δεκαεξαδική μορφή, η οποία επιτρέπει όχι μόνο αριθμούς (0-9), αλλά και μερικούς χαρακτήρες, (a-f). Για παράδειγμα μια διεύθυνση IPv6 έχει την μορφή 3ffe: ffff: 100: F101: 210: a4ff: fee3: 9566.

Υπάρχουν δύο σημαντικές βελτιώσεις στο IPv6 σε σχέση με το IPv4:

- Σημειώνεται σημαντική βελτίωση στην επεκτασιμότητα και στις επιλογές του πρωτοκόλλου διαδικτύου νέας γενιάς. Οι επιλογές τοποθετούνται σε ξεχωριστές επικεφαλίδες που βρίσκονται μεταξύ της επικεφαλίδας του IPv6 και της επικεφαλίδας του επιπέδου μεταφοράς. Υπάρχουν αλλαγές στον τρόπο με τον οποίο κωδικοποιούνται οι επιλογές στην επικεφαλίδα IP επιτυγχάνοντας, **αποτελεσματικότερη προώθηση**, λιγότερο αυστηρά όρια όσο αφορά το μήκος των επιλογών καθώς και **μεγαλύτερη ευελιξία για την εισαγωγή νέων επιλογών στο μέλλον.**
- Προστίθεται μια **νέα δυνατότητα (Flow label)** με την οποία επισημαίνονται όλα τα πακέτα που ανήκουν σε συγκεκριμένη ροή κυκλοφορίας, για τα οποία ο αποστολέας έχει ζητήσει ειδική μεταχείριση, όπως non-default Quality of Services ή real-time services. [17]



Εικόνα 5:Δομή πρωτοκόλλου IPv6 χωρίς επικεφαλίδες επέκτασης.

Η δομή της επικεφαλίδας του IPv6 δίνεται στην εικόνα 5. Στο IPv6 υπάρχουν δύο είδη κεφαλίδων. Η main/regular IPv6 και η IPv6 extension header. Παρακάτω αναλύονται **τα πεδία της επικεφαλίδας του πρωτοκόλλου IPv6.**

- ***Version***

Αναφέρεται στην έκδοση του πρωτοκόλλου IP και αποτελείται από 4 bits.

- ***Priority ή Traffic Class***

Είναι παρόμοιο με το Type of Services του πρωτοκόλλου IPv4. Ορίζει το είδος της υπηρεσίας που ανήκει στο μοντέλο διαφορετικών υπηρεσιών που πρέπει να δοθεί στο πακέτο. Αποτελείται από 8-bit και προσδιορίζει την επιθυμητή προτεραιότητα παράδοσης των πακέτων. Είχε οριστεί για πρώτη φορά σαν πεδίο Priority. Κατόπιν το όνομα αλλάχτηκε σε Class και πρόσφατα χαρακτηρίζεται σαν Traffic class.

- ***Flow Label***

Χρησιμοποιείται για να αναγνωριστούν τα πακέτα της ίδιας ροής. Ένας κόμβος μπορεί να έχει περισσότερες από μία ροές πακέτων. Αποτελείται από 20-bit. Χρησιμοποιείται από μια πηγή για να

επισημάνει τα πακέτα που ανήκουν στην ίδια ροή και ζητά ειδική μεταχείριση από το δρομολογητή IPv6.

- ***Payload length***

Είναι ένας αριθμός (16 bits) που δηλώνει το μήκος του πακέτου των δεδομένων, δηλαδή του πακέτου μετά το τέλος των επικεφαλίδων (payload) σε bytes. Περιλαμβάνει και το μέγεθος των IPv6 header extensions εάν υπάρχουν.

- ***Next header***

Αποτελείται από 8 bits και αναφέρει πιο πρωτόκολλο χρησιμοποιείται στην επικεφαλίδα μετά το IPv6 πακέτο. Εκτός από το να αναφέρεται σε κάποιο ανώτερου επιπέδου πρωτόκολλο όπως τα TCP και UDP, μπορεί να αναφέρει την ύπαρξη IPv6 extension headers.

- ***Hop limit***

Είναι ένας ακέραιος των 8-bits ο οποίος κάθε φορά που ένας κόμβος προωθεί το πακέτο, μειώνει το μέγεθος του κατά ένα. Όταν αυτό μηδενιστεί το πακέτο διαγράφεται από το δίκτυο.

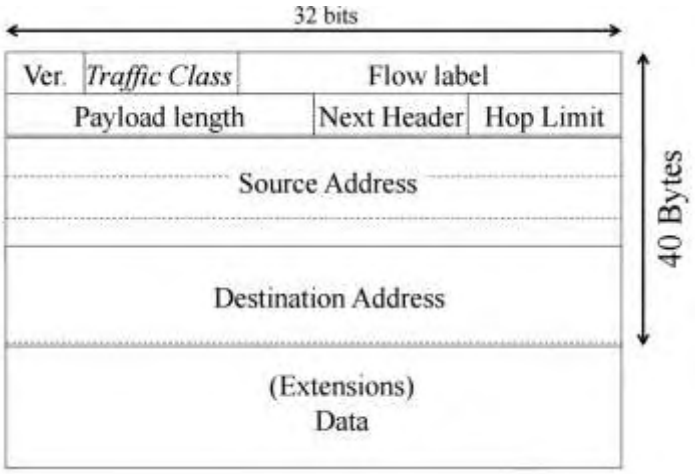
- ***Source address***

Είναι η IPv6 διεύθυνση του κόμβου που δημιούργησε το πακέτο και είναι ένα πεδίο των 128-bits.

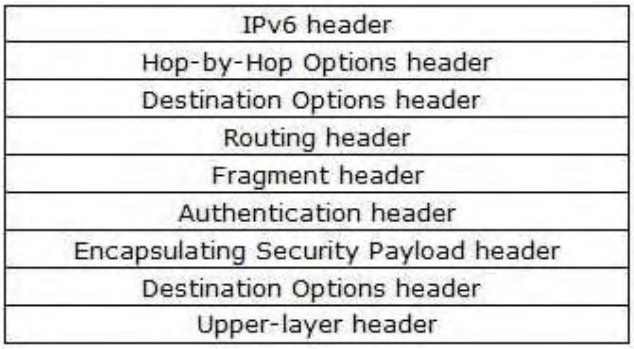
- ***Destination address***

Είναι η IPv6 διεύθυνση του κόμβου ή των κόμβων που πρόκειται να παραλάβουν το πακέτο. Μπορεί να είναι διεύθυνση τύπου unicast, multicast ή anycast. Εάν στο πακέτο υπάρχει και routing extension που ορίζει το μονοπάτι που πρέπει να ακολουθήσει το πακέτο, τότε η διεύθυνση προορισμού μπορεί να είναι ένας από τους ενδιάμεσους κόμβους αντί αυτής που αναφέρεται στο πεδίο διεύθυνση παραλήπτη (128-bits).

Στο πρωτόκολλο IPv6 οι επικεφαλίδες είναι οργανωμένες σε λέξεις των 64 bits και το συνολικό μέγεθος των επικεφαλίδων είναι 40 bytes. Επιπλέον, στο IPv6 μπορούν να υπάρχουν προαιρετικά επικεφαλίδες επέκτασης που θα πρέπει να εμφανίζονται με συγκεκριμένη σειρά. Η κάθε επικεφαλίδα αναφέρει ποια είναι η επόμενη επικεφαλίδα που ακολουθεί ή αν είναι η τελευταία. [20]



Εικόνα 6: Δομή πρωτοκόλλου IPv6 με επικεφαλίδες επέκτασης.



Εικόνα 7: Οι επικεφαλίδες επέκτασης.

- ***Hop-by-Hop Options Header***

Αυτή η επικεφαλίδα ακολουθεί πάντα την επικεφαλίδα του IPv6 πακέτου. Περιλαμβάνει δεδομένα τα οποία θα πρέπει να επεξεργαστεί κάθε κόμβος στον οποίο φτάνει το πακέτο.

- ***Destination Options Header***

Περιέχει πληροφορίες που θα πρέπει να ελεγχθούν από τον πρώτο παραλήπτη που αναφέρεται στη διεύθυνση προορισμού και στις διευθύνσεις που περιλαμβάνονται στο Routing Header.

- ***Routing Header***

Αναφέρονται οι διάφοροι κόμβοι που θα επισκεφτεί το πακέτο κατά τη διαδρομή από τον αποστολέα στον παραλήπτη. Ο κάθε κόμβος που παραλαμβάνει το πακέτο ελέγχει ποιος είναι ο επόμενος παραλήπτης στη λίστα και προωθεί το πακέτο σ' αυτόν.

- ***Fragment Header***

Χρησιμοποιείται από τον κόμβο αποστολέα προκειμένου να μεταδώσει πακέτα με μέγεθος μεγαλύτερο από το μέγιστο επιτρεπόμενο μέγεθος πακέτου (Path MTU) στο μονοπάτι από τον αποστολέα στον παραλήπτη.

- ***Authentication Header***

Χρησιμοποιείται προκειμένου να εξασφαλιστεί ότι τα δεδομένα δεν έχουν αλλαχτεί κατά τη μετάδοση του πακέτου στο μονοπάτι από τον αποστολέα στον παραλήπτη. Η μέθοδος που χρησιμοποιείται για αυτό είναι ένα κρυπτογραφημένο checksum κάποιων από τις επικεφαλίδες του IPv6 και των δεδομένων (payload).

- ***Encapsulating Security Payload Header***

Πρόκειται για την τελευταία επικεφαλίδα που μπορεί να υπάρξει στη σειρά των επικεφαλίδων επέκτασης που δεν έχει κωδικοποιηθεί (αν έχει επιλεγεί από τον κόμβο αποστολέα η κωδικοποίηση των δεδομένων που μεταδίδει). Χρησιμοποιείται προκειμένου να δείξει ότι ολόκληρο το πακέτο έχει κωδικοποιηθεί και παρέχει πληροφορία για τον κόμβο παραλήπτη για τη διαδικασία αποκρυπτογράφησης.

- ***Destination Options Header***

Αντιστοιχεί στο πεδίο IP Options του IPv4. Ο κόμβος παραλήπτη επεξεργάζεται αυτήν την επικεφαλίδα αφού παραλάβει το πακέτο. Προς το παρόν δε χρησιμοποιείται καθόλου αυτό το πεδίο και απλώς συμπληρώνεται με bits (padding).

Όλες οι επικεφαλίδες στο IPv6 έχουν το ίδιο μέγεθος και την ίδια μορφοποίηση. Η διαφορά τους βρίσκεται στο πεδίο που αφορά την επόμενη επικεφαλίδα. Η σειρά με την οποία μπορούν να εμφανίζονται οι επικεφαλίδες είναι αυστηρά καθορισμένη. [21]

Στον πίνακα 2 δίνονται οι βασικές διαφορές μεταξύ των πρωτοκόλλων IPv4 και IPv6. [22]

	IPv4	*IPv6*
Χώρος	32 bits	128 bits
Υποστήριξη IPsec	Προαιρετική	Απαιτούμενη
Options	Στην επικεφαλίδα	Επικεφαλίδα Επέκτασης
CheckSum	Ναι	Όχι
Κατακερματισμός	Γίνεται από την αποστολή υποδοχής και τους δρομολογητές	Γίνεται μόνο από την αποστολή υποδοχής
Broadcast	Ναι	Όχι
Μέγεθος πακέτου	576 bytes	1280 bytes
DNS	Χρήση διεύθυνσης (A)	Χρήση διεύθυνσης (AAAA)
IGMP	Διαχειρίζεται τα τοπικά μέλη της ομάδας	Αντικαταστάθηκε με το MLD
ARP	Χρησιμοποιείται για την μετάδοση πλαισίων μιας link-layer διεύθυνσης	Έχει αντικατασταθεί με τα μηνύματα multicast Neighbor Solicitation
PTR	Χρησιμοποιείται για την εγγραφή πόρων και διευθύνσεων στο IN-ADDR.ARPA DNS	Χρησιμοποιείται για την εγγραφή πόρων και διευθύνσεων στο IPv6-ADDR.ARPA DNS
ICMP	Χρησιμοποιείται	Δεν χρησιμοποιείται
Διαμόρφωση IP	Χειροκίνητη ή με DHCP	Autoconfiguration
Πακέτα ροής QoS	Δεν εντοπίζονται	Τα χειρίζεται

Πίνακας 2: Διαφορές μεταξύ IPv4 και IPv6.

2.3.2 Τεχνολογία MPLS (Multi-Protocol Label Switching)

Η αντιμετώπιση των προβλημάτων αξιοπιστίας και ποιότητας υπηρεσίας του παραδοσιακού IP σίγουρα δεν μπορεί να γίνει με την εισαγωγή μιας νέας τεχνολογίας που θα το αντικαταστήσει και δε θα λάβει υπόψη την υπάρχουσα εγκατεστημένη βάση των υπηρεσιών και εφαρμογών που χρησιμοποιούνται ευρέως.. Και αυτό διότι οποιαδήποτε νέα τεχνολογία που θα αναπτυχθεί και η οποία δεν θα υποστηρίζει τα υφιστάμενα IP πρωτόκολλα και εφαρμογές, δεν θα μπορέσει πιθανότατα να γίνει αποδεκτή από την αγορά. Η τεχνολογία MPLS έχει αποφύγει αυτό τον σκόπελο και **καταφέρνει να αναπτύσσεται διατηρώντας την συμβατότητα, τη συνεργασία και την υποστήριξη όλων των γνωστών πρωτοκόλλων.** Με την υπηρεσία MPLS VPN επιτυγχάνεται η διασύνδεση δύο ή περισσότερων επιχειρηματικών κέντρων ενός πελάτη συνδυάζοντας την μεταφορά δεδομένων, φωνής, video και multimedia πάνω από μία ενοποιημένη πλατφόρμα βασισμένη στην IP τεχνολογία. Το Multiprotocol Label Switching (MPLS) είναι ένα πρωτόκολλο που δημιουργήθηκε από την IETF. Συνδυάζει την μεταγωγή με ετικέτα (label) και την παραδοσιακή δρομολόγηση του IP, με στόχο να αυξήσει την ευελιξία και την απόδοση του πρωτοκόλλου IP, και ταυτόχρονα να δώσει την δυνατότητα για την παροχή νέων υπηρεσιών στο Internet. Έτσι, ενώ το

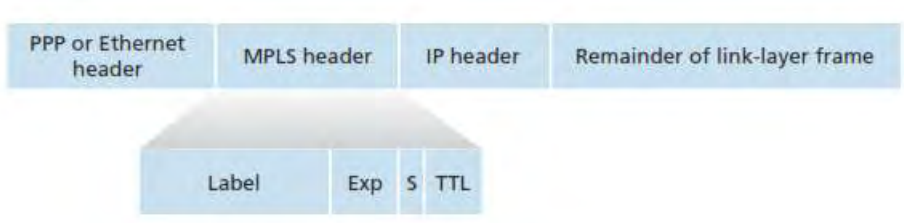
MPLS συνεργάζεται με τα υφιστάμενα πρωτόκολλα, επιτρέπει την μεταγωγή με κύκλωμα στο Internet.

Η μεταγωγή με ετικέτα (label) επιτυγχάνεται τοποθετώντας στην αρχή κάθε πακέτου, κατά την είσοδό του στο δίκτυο MPLS, μια ετικέτα. Η απόφαση για το πώς θα δρομολογηθεί το πακέτο εξαρτάται μόνο από αυτή την ετικέτα και όχι από την διεύθυνση IP. Η ετικέτα απομακρύνεται κατά την έξοδο του πακέτου από το δίκτυο MPLS. Οι δρομολογητές οι οποίοι χρησιμοποιούν την μεταγωγή με ετικέτα (label) ονομάζονται **Label Switching δρομολογητές (LSRs).**

Οι συσκευές οι οποίες συμμετέχουν στους μηχανισμούς του πρωτοκόλλου MPLS μπορούν να ταξινομηθούν σε ακραίους δρομολογητές ετικέτας Label Edge Routers (LERs) και δρομολογητές μεταγωγής ετικέτας Label Switching Routers (LSRs).

Το MPLS εκτός από τους δρομολογητές ετικέτας (LSRs), απαιτεί τη χρήση και Ακραίων Δρομολογητών Ετικέτας Label Edge Routers (LERs). Ο LER είναι ένας δρομολογητής ο οποίος λειτουργεί στο άκρο μεταξύ του δικτύου πρόσβασης και του MPLS δικτύου. Υποστηρίζουν πολλαπλές θύρες συνδεδεμένες σε διαφορετικά δίκτυα (όπως Frame Relay και Ethernet) και προωθεί την κυκλοφορία πάνω στο MPLS δίκτυο, χρησιμοποιώντας πρωτόκολλο σηματοδοσίας ετικέτας κατά την είσοδο και κατανέμοντας την κυκλοφορία πίσω στα δίκτυα πρόσβασης στην έξοδο. Ο ακραίος δρομολογητής ετικέτας (LER) διαδραματίζει σημαντικό ρόλο στην ανάθεση και αφαίρεση των ετικετών, κατά την είσοδο ή έξοδο της κυκλοφορίας από ένα MPLS δίκτυο.

Η τοποθέτηση της επικεφαλίδας MPLS ανάμεσα στο εκάστοτε επίπεδο σύνδεσης (π.χ. PPP, ethernet) και στο επίπεδο δικτύου οτυ διαδικτύου (IP) φαίνεται στην παρακάτω εικόνα.



Εικόνα 8: Επικεφαλίδα MPLS.

Το πρωτόκολλο MPLS εκτελεί γενικά τις ακόλουθες λειτουργίες. Καθορίζει τους απαραίτητους μηχανισμούς για τη διαχείριση της ροής κυκλοφορίας των διάφορων στοιχείων ενός δικτύου, παραμένει ανεξάρτητο από τα πρωτόκολλα του 2^{ου} και 3^{ου} επιπέδου του OSI (όπως φαίνεται και στην παραπάνω εικόνα) και παρέχει τα μέσα για την αντιστοίχηση των διευθύνσεων IP σε απλές καθορισμένου μήκους ετικέτες (labels) που χρησιμοποιούνται από διαφορετικές τεχνολογίες προώθησης και μεταγωγής πακέτων (packet-forwarding & packet-switching). Συνεργάζεται με τα υπάρχοντα πρωτόκολλα δρομολόγησης και υποστηρίζει τα πρωτόκολλα επιπέδου 2. Η υλοποίηση των MPLS VPNs σήμερα γίνεται με τη συνεργασία δύο πρωτοκόλλων, του MPLS και του BGP (Border Gateway Protocol), όπου το MPLS χρησιμοποιείται για την προώθηση των πακέτων στο δίκτυο και το BGP για τη διανομή των διαδρομών (κατ' επέκταση των ετικετών).

Γενικά, για να γίνει αυτό εφικτό απαιτούνται η ελεγχόμενη διανομή των πληροφοριών δρομολόγησης (Constrained Distribution), πολλαπλοί πίνακες προώθησης, νέοι τύποι διευθύνσεων και οι μηχανισμοί προώθησης του MPLS.

Ελεγχόμενη διανομή των πληροφοριών δρομολόγησης

Με έλεγχο του τρόπου διανομής των πληροφοριών δρομολόγησης (πίνακες δρομολόγησης), ελέγχουμε ουσιαστικά την ροή των δεδομένων στο δίκτυο. Η πληροφορία διαδίδεται από τον Ακραίο Δρομολογητή του Πελάτη "Customer Edge device"(CE) στον Ακραίο Δρομολογητή του Δικτύου του Παρόχου "Provider Edge device" (PE), με τον οποίο είναι συνδεδεμένος. Στη συνέχεια, από τον εισερχόμενο PE δρομολογητή, η πληροφορία αναδιανέμεται στο BGP του παρόχου και η πληροφορία δρομολόγησης διανέμεται ανάμεσα στους υπόλοιπους PE δρομολογητές του δικτύου. Στους εξερχόμενους PE δρομολογητές η πληροφορία δρομολόγησης εισάγεται από το BGP του παρόχου και η πληροφορία δρομολόγησης αποστέλλεται από τον PE δρομολογητή εξόδου στον CE δρομολογητή.

Η ελεγχόμενη διανομή των πληροφοριών δρομολόγησης γίνεται με χρήση της τεχνικής φιλτραρίσματος με βάση την ιδιότητα "Community" του BGP. Ο PE δρομολογητής εισάγει μία κατάλληλη τιμή στο πεδίο Community, πριν εξάγει τις πληροφορίες δρομολόγησης στο BGP. Ο PE δρομολογητής εξόδου, χρησιμοποιώντας την τιμή του BGP Community, ελέγχει την διανομή των πληροφοριών δρομολόγησης στον CE δρομολογητή. Η λειτουργία αυτή ελέγχεται αποκλειστικά από τον πάροχο και ο πελάτης δεν χρειάζεται να γνωρίζει κάτι, ή να εμπλακεί με κάποια σχετική ενέργεια.

Πολλαπλοί πίνακες προώθησης

Επειδή ένας PE δρομολογητής ελέγχει συνήθως πολλά διαφορετικά VPNs, η διατήρηση ενός κοινού πίνακα δρομολόγησης για όλα τα εικονικά δίκτυα αποτρέπει τον διαχωρισμό της πληροφορίας δρομολόγησης, με αποτέλεσμα να είναι πιθανή η προώθηση πακέτων μεταξύ διαφορετικών VPNs.

Η αντιμετώπιση του παραπάνω προβήματος γίνεται με την υποστήριξη πολλαπλών πινάκων δρομολόγησης σε κάθε PE δρομολογητή. Δηλαδή, υπάρχει ένας πίνακας δρομολόγησης για κάθε ένα VPN.

Οι μηχανισμοί προώθησης του *MPLS-VPN*

Το καθοριστικό πλεονέκτημα του MPLS, στην προκειμένη περίπτωση, είναι ο διαχωρισμός της πληροφορίας προώθησης (ετικέτα) από την επικεφαλίδα – header (IP διεύθυνση) του IP πακέτου που εφαρμόζει.

Για την υποστήριξη των IP-VPNs διευθύνσεων από το MPLS χρησιμοποιείται η τεχνική του label stack, δηλαδή κάθε πακέτο φέρει δύο ετικέτες. Η ετικέτα που βρίσκεται στην κορυφή της στοίβας (δεύτερο επίπεδο) συσχετίζεται με τους PE δρομολογητές εισόδου/εξόδου και υλοποιεί έτσι τον μηχανισμό προώθησης από έναν PE δρομολογητή εισόδου σε έναν PE δρομολογητή εξόδου. Η ετικέτα του πρώτου επιπέδου ελέγχει την προώθηση στον PE δρομολογητή εξόδου. Οι ετικέτες αυτού του επιπέδου διανέμονται αποκλειστικά μέσω του BGP μαζί με τις IP-VPN διευθύνσεις.

Όταν μία IP-VPN διεύθυνση (δηλαδή μια διεύθυνση πελάτη) διανέμεται μέσω του BGP, μεταφέρει ως τιμή την διεύθυνση του PE δρομολογητή που την δημιούργησε (και όχι την διεύθυνση του CE δρομολογητή). Αυτή η διεύθυνση του PE δρομολογητή είναι προφανώς μια συνηθισμένη IP διεύθυνση του δικτύου του παρόχου και δρομολογείται σύμφωνα με κάποια διαδικασία δρομολόγησης. [23]**.**

2.3.3 Layer 2 Tunneling Protocol (L2TP)

Το L2TP παρέχει συμπίεση βασισμένη στο λογισμικό η οποία **συμπυκνώνει τα πακέτα των χρηστών**. Επίσης, ένας μικρός αριθμός τεχνικών συμπίεσης έχει προστεθεί στο επίπεδο της κρυπτογράφησης. Το L2TP χρησιμοποιεί δύο συναρτήσεις: την client-like line server η οποία αναφέρεται ως **LAC (L2TP Access Concentrator)** και είναι ένας L2TP συγκεντρωτής πρόσβασης και τον server-side network server ο οποίος καλείται LNS **(L2TP Network Server)**. Όταν ένα PC κάνει PPP σύνδεση στον ISP, μία LAC συνάρτηση αρχικοποιεί το tunnel, προσθέτει διάφορους headers στο PPP payload και εγκαθιδρύει το tunnel στην LNS τερματική συσκευή – αυτή η συσκευή μπορεί να είναι router, server ή συσκευή πρόσβασης. Αφού έχει εγκαθιδρυθεί το tunnel, εγκαθίσταται ένας μηχανισμός πιστοποίησης του χρήστη για να πιστοποιείται η ταυτότητα των χρηστών. Επίσης, το L2TP χρησιμοποιεί control μηνύματα για την βελτιστοποίηση του tunnel.

Το **L2TP** είναι ένα πρωτόκολλο **2^{ου} επίπεδου** σχεδιασμένο για το encapsulation στο επίπεδο αυτό. Επομένως, το **IPSec,** το οποίο είναι ένα **πρωτόκολλο 3^{ου} επιπέδου,** μπορεί **να χρησιμοποιηθεί μαζί με το L2TP για** περισσότερη **ασφάλεια** (στην πραγματικότητα αυτό συνίσταται). [24]

ΚΕΦΑΛΑΙΟ 3: ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ VPNs

Οι αρχιτεκτονικές των VPNs μπορούν να οριστούν σε συνάρτηση με τη χρήση του VPN, την αρχιτεκτονική του και τις τεχνολογιές ή τα πρωτόκολλα που χρησιμοποιούνται για την υλοποίησής τις λογικής σύνδεσης τους.

Στο κεφάλαιο αυτό θα αναλύσουμε τις αρχιτεκτονικές των VPNs και θα εμβαθύνουμε στο τρόπο υλοποίησής τους.

3.1 Κατηγοροιοποίηση VPNs με βάση τη χρήση τους

Τα ιδιωτικά εικονικά δίκτυα από πλευράς χρήσης μπορούν να διακριθούν σε **remote access** και σε **site to site** VPN.

Στα remote access VPN δύο από τις πιο κοινές αρχιτεκτονικές VPN είναι το Layer 2 Tunneling Protocol (L2TP) και το IPSec.

Το L2TP είναι ένα πρότυπο IETF (RFC 2661) για τη μεταφορά PPP frames πάνω από IP/UDP.

Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την **ασφαλή μετάδοση και ανταλλαγή δεδομένων** (packets) **μέσω του στρώματος IP**. Το IPsec αποτελεί ένα από τους πιο διαδεδομένους τρόπους υλοποίησης VPNs και θα εξεταστεί με λεπτομέρια στη συνέχεια.

Στα site to site VPN οι τεχνολογίες που χρησιμοποιούνται είναι συνήθως Frame Relay, Asynchronous Transfer Moded (ATM), Generic Routing Encapsulation (GRE) και Multi-Protocol Label Switching (MPLS). Το κοινό γνώρισμα αυτών των μεθόδων είναι ότι μπορούν να προσφέρουν κάποιο είδος εγγύησης ποιότητα υπηρεσίας (Quality of Service, QoS). Το MPLS αποτελεί ένα από τους πιο διαδεδομένους τρόπους υλοποίησης VPNs και θα εξεταστεί με λεπτομέρια στη συνέχεια.

3.2 Διάκριση VPN με βάση τη αρχιτεκτονική τους

Μια διαφορετική διάκριση των Virtual Private Network ως προς την αρχιτεκτονική τους είναι η εξής:

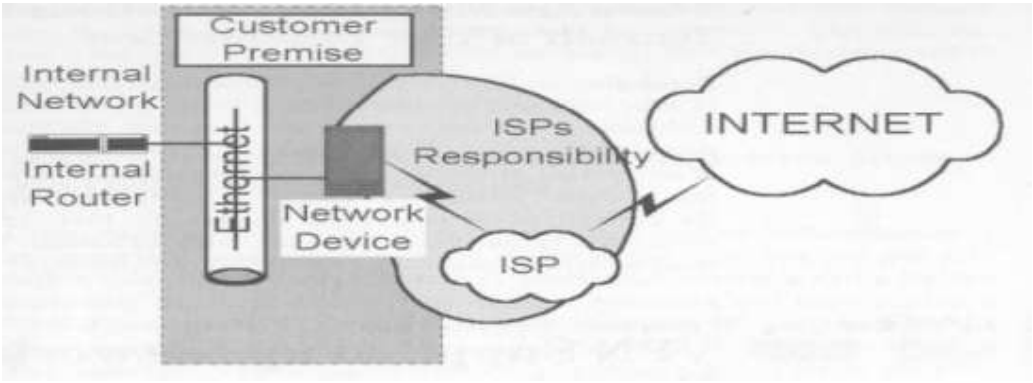
- Τα VPN που υποστηρίζονται από τον παροχέα δικτυακών υπηρεσιών (NSP)
- Τα VPN που βασίζονται στο firewall
- Τα VPN που βασίζονται στο black-box
- Τα VPN που βασίζονται στο δρομολογητή (router)
- Τα VPN που βασίζονται στην απομακρυσμένη σύνδεση
- Τα VPN των application aware
- Τα VPN που βασίζονται στο λογισμικό
- Τα VPN multiservice application και τα tunnel switching

3.2.1 Τα VPN που υποστηρίζονται από τον παροχέα δικτυακών υπηρεσιών (Network Service Providers - NSP)

Τα εικονικά ιδιωτικά δίκτυα που υποστηρίζονται από τον παροχέα αποτελούν μία από τις πιο διαδεδομένες μορφές VPN στη σημερινή εποχή και είναι αρκετές οι επιχειρήσεις που την ακολουθούν στην προσπάθεια τους να εκμεταλλευτούν τις δυνατότητες των VPN ενώ ταυτόχρονα είναι συνδεδεμένες με το Διαδίκτυο. Σύμφωνα με τη συγκεκριμένη αρχιτεκτονική **ο παροχέας** δικτυακών υπηρεσιών συνήθως (NSP) αναλαμβάνει **να εγκαταστήσει κάποια συσκευή VPN** για λογαριασμό της επιχείρησης πελάτη η οποία θα δημιουργεί τα tunnels κάθε φορά που θα απαιτείται κάποια εικονική σύνδεση. Τα **πακέτα πληροφορίας θα κρυπτογραφούνται από τη συσκευή** αυτή, όπως επίσης και θα αποκρυπτογραφεί τα αποστελλόμενα πακέτα δεδομένων προς τον υπολογιστή Host της επιχείρησης. Συνήθως, τοποθετείται κάποιο τοίχος πυρασφάλειας **(firewall)** ακριβώς μπροστά από τη συσκευή VPN με στόχο τη μεγαλύτερη προστασία των μεταδιδόμενων πληροφοριών.

Όσον αφορά στην συνδεσμολογία, από τη μια μεριά του firewall συνδέεται ο εσωτερικός δρομολογητής του τοπικού δικτύου της επιχείρησης, ενώ από την άλλη μεριά του firewall, συνδέεται ένας εξωτερικός δρομολογητής, ο οποίος με τη σειρά του συνδέεται με τον παροχέα διαδικτυακών υπηρεσιών. Οι οργανισμοί που επιλέγουν μία αρχιτεκτονική ενός Εικονικού Ιδιωτικού Δικτύου το οποίο υποστηρίζεται από τον παροχέα δικτυακών υπηρεσιών, ενδιαφέρονται κυρίως για την διεξαγωγή τηλε-συνδιασκέψεων (teleconferencing) ή ακόμη θέλουν να επωφεληθούν από τις δυνατότητες της IP τηλεφωνίας, δηλαδή του τηλεφώνου μέσω Διαδικτύου.

Κύριο μειονέκτημα της αρχιτεκτονικής αυτής είναι η **περιορισμένη δυνατότητα αναβάθμισης του Εικονικού Ιδιωτικού Δικτύου με περισσότερες υπηρεσίες**. Κάθε φορά που μια επιχείρηση-πελάτης ζητά αναβάθμιση του VPN της, οι NSPs παρότι είναι μεγάλοι οργανισμοί και υποστηρίζουν ταυτόχρονα μια πληθώρα από VPN συνδέσεις, δυσκολεύονται σε μεγάλο βαθμό πραγματοποιήσουν αναβάθμιση λόγω του μεγάλου πλήθους συνδέσεων και των διαφορετικών απαιτήσεων του πελάτη. Στην παρακάτω εικόνα απεικονίζεται μια αρχιτεκτονική VPN η οποία υποστηρίζεται από τον παροχέα δικτυακών υπηρεσιών ISP (Internet Service Provider) η οποία δίνει την πρόσβαση στο διαδίκτυο. [25]



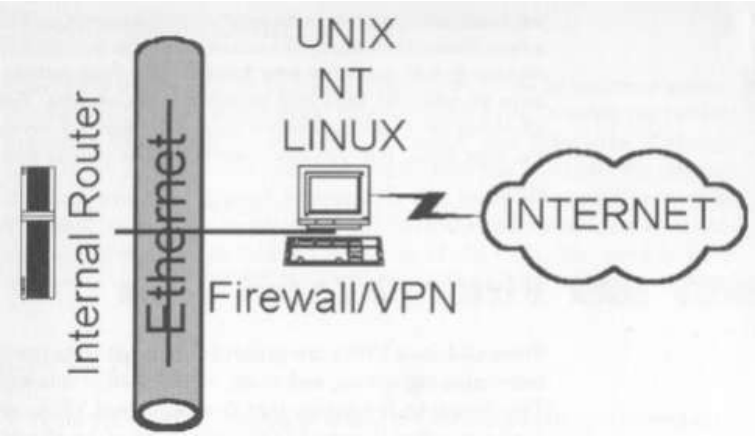
Εικόνα 9: Αρχιτεκτονική VPN που υποστηρίζεται από τον παροχέα δικτυακών υπηρεσιών ISP.

3.2.2 VPNs που βασίζονται στο τείχος προστασίας (firewall)

Τα τελευταία χρόνια σχεδόν όλες οι επιχειρήσεις, μεγάλες και μικρές, προστατεύουν τα δίκτυα τους με τη χρήση κάποιου τείχους προστασίας (firewall). Η αρχιτεκτονική του Εικονικού Ιδιωτικού Δικτύου που βασίζεται στο firewall **αποτελεί μια από τις πιο διαδεδομένες**. Απαραίτητη προϋπόθεση για τη δημιουργία ενός VPN με την αρχιτεκτονική αυτή, είναι **η υποστήριξη του απαραίτητου λογισμικού κρυπτογράφησης από το ίδιο το firewall.** Τις περισσότερες φορές οι ίδιοι οι κατασκευαστές των firewalls προσφέρουν χωρίς επιπλέον κόστος, μαζί με το προϊόν και επιπλέον ένα λογισμικό κρυπτογράφησης. Υπάρχει βέβαια η δυνατότητα μία επιχείρηση να επιλέξει εκ των υστέρων ξεχωριστά ένα διαφορετικό λογισμικό, το οποίο θα έχει δυνατότητες κρυπτογράφησης και θα καλύπτει τις απαιτήσεις της.

Υπάρχουν δίκτυα τα οποία βασίζονται σε διαφορετικές τεχνολογίες όπως σε UNIX ή δίκτυα με διαφορετική τοπολογία, δηλαδή η μορφή της σύνδεσης μεταξύ των κόμβων του δικτύου είναι διαφορετική. Ένα βασικό χαρακτηριστικό των firewalls είναι η συμβατότητα τους με τις διάφορες αρχιτεκτονικές δικτύου. Παρότι η διάδοση των firewalls είναι μεγάλη και η αποτελεσματικότητα ως προς την ασφάλεια ενός δικτύου είναι μεγάλη, δεν θα πρέπει να θεωρούνται απόλυτα ασφαλείς. Ένα προβληματικό και επιρρεπές λειτουργικό σύστημα σε hackers ταυτόχρονα καθιστά προβληματικό και το firewall.

Πολλά firewalls εκτός από το τείχος προστασίας, παρέχουν υποστήριξη Εικονικού Ιδιωτικού Δικτύου. **Διαχειρίζονται** με αυτόν τον τρόπο **ολόκληρη την κυκλοφορία των IP πακέτων και επιτρέπουν ή απορρίπτουν την πρόσβαση δεδομένων προς το δίκτυο ανάλογα με τα φίλτρα προστασίας που υποστηρίζουν**. Τα **μεγάλα δίκτυα** χαρακτηρίζονται από **υψηλή κίνηση πληροφορίας** και απαιτούν συχνή αναβάθμιση για το λόγο αυτό **χρησιμοποιούν τα firewalls που υποστηρίζουν το μηχανισμό tunneling,** ενώ τα μικρότερα δίκτυα (1-2 Mbps WANs) χρησιμοποιούν την υποστήριξη τόσο του tunneling, όσο και του μηχανισμού κρυπτογράφησης καθώς δεν υπάρχει υψηλή κίνηση πληροφορίας και δεν απαιτούν συχνή αναβάθμιση. Η παρακάτω εικόνα απεικονίζει μια αρχιτεκτονική VPN η οποία βασίζεται σε ένα firewall. [26]



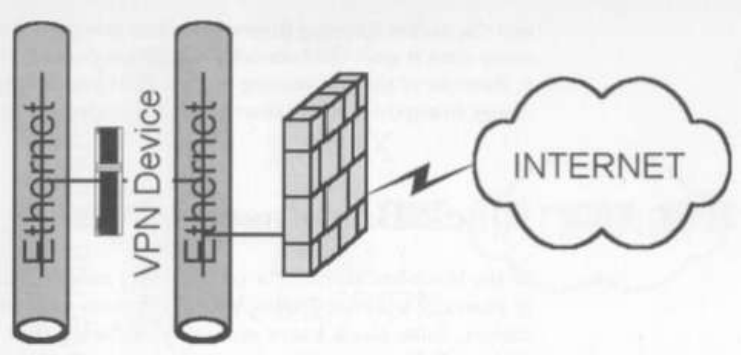
Εικόνα 10: Αρχιτεκτονική VPN που βασίζεται σε firewall.

3.2.3 VPNs που βασίζονται στο black-box

Το black-box είναι μία συσκευή δικτύου, η οποία διαθέτει ένα λογισμικό κρυπτογράφησης **και βασική λειτουργία της είναι να δημιουργήσει tunnels εικονικού δικτύου**. Αυτή η μορφή VPN χρησιμοποιεί μια **συσκευή black-box** η οποία είναι συνδεδεμένη στο δίκτυο και μπορεί να διαχειρίστεί είτε από κάποιο επιτραπέζιο υπολογιστή – client δεδομένου του αντίστοιχου λογισμικού υποστήριξης είτε από κάποιο browser ο οποίος μπορεί να διαχειρίζεται τα black-box μέσω του δικτύου.

Ένα βασικό χαρακτηριστικό της αρχιτεκτονικής των black-box συσκευών, είναι ότι **παρουσιάζουν συμβατότητα με όλα τα πρωτόκολλα tunneling**. Από την άλλη πλευρά, οι συσκευές αυτές **δεν παρέχουν ασφάλεια** στα δίκτυα, με αποτέλεσμα οι επιχειρήσεις να πρέπει να εγκαταστήσουν κάποιο **ξεχωριστό τείχος ασφάλειας**. Τα τελευταία χρόνια άρχισαν να διατίθενται στην αγορά και συσκευές black-box που ενσωμάτωναν και τις δυνατότητες ενός firewall.

Γενικά, υπάρχουν αρκετές αρχιτεκτονικές VPN που είναι παρόμοιες με τον τρόπο λειτουργίας μιας συσκευής black-box, γι' αυτό ονομάζονται **αρχιτεκτονικές τύπου Hardware**. Όσο αφορά στην λειτουργία τους, οι συσκευές εικονικού δικτύου είναι περιφερειακές συσκευές οι οποίες συνήθως λειτουργούν ως **γέφυρες (Bridges) που αναλαμβάνουν την κρυπτογράφηση**. Τοποθετούνται μεταξύ των δρομολογητών του δικτύου. Στην παρακάτω εικόνα απεικονίζεται μια αρχιτεκτονική η οποία βασίζεται σε συσκευή black-box. [26]



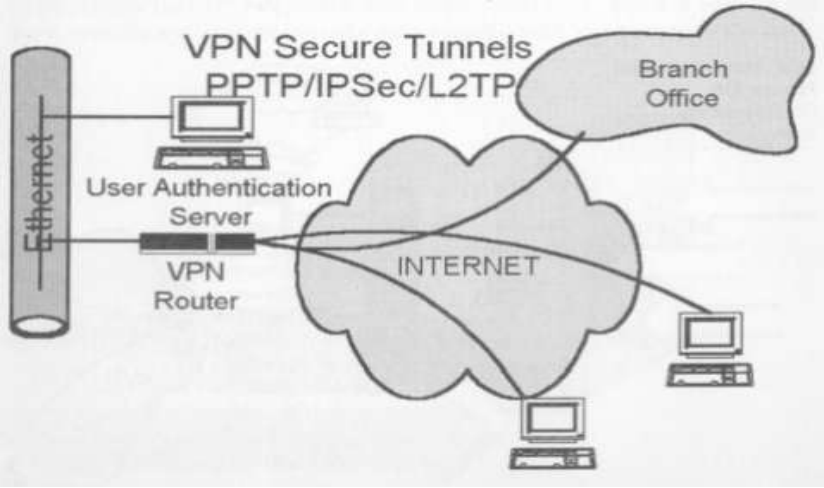
Εικόνα 11: Αρχιτεκτονική VPN που βασίζεται στο black-box.

3.2.4 VPNs που βασίζονται στο δρομολογητή (Router)

Βασική λειτουργία του δρομολογητή σε μία αρχιτεκτονική Εικονικού Ιδιωτικού Δικτύου είναι **να ελέγχει κάθε πακέτο πληροφορίας που δρομολογείται εντός του δικτύου καθώς και να υποστηρίζει τον μηχανισμό της κρυπτογράφησης του κάθε πακέτου δεδομένων.**

Η υλοποίηση εικονικών δικτύων που βασίζονται στο δρομολογητή (router), μπορεί να γίνει με δύο τρόπους. Ο πρώτος τρόπος αφορά στην **ενσωμάτωση κατάλληλου λογισμικού στον ήδη υπάρχοντα δρομολογητή του δικτύου,** ο οποίος αναλαμβάνει να κρυπτογράφησει τα πακέτα που ανταλάσσονται. Ο **δεύτερος τρόπος** υλοποίησης ενός vpn μέσω της αρχιτεκτονικής router είναι η **ενσωμάτωσης μιας εξωτερικής κάρτας με διάφορα κυκλώματα (circuits) εντός της συσκευής του router.** Η εξωτερική αυτή κάρτα περιλαμβάνει μία κεντρική μονάδα επεξεργασίας **(CPU)** και σκοπός της είναι να αναλάβει τη διαδικασία της κρυπτογράφησης.

Όσο περισσότεροι χρήστες συνδέονται στο Εικονικό Δίκτυο, τόσο μεγαλύτερη πρέπει να είναι η επεξεργαστική ισχύς του δρομολογητή. Στις περιπτώσεις αυτές χρησιμοποιείται η ενσωμάτωση της εξωτερικής κάρτας πάνω στο router η οποία διαθέτει μεγάλη επεξεργαστική ισχύς. Βέβαια εάν μια επιχείρηση η οποία θέλει να δημιουργήσει το εικονικό ιδιωτικό της δίκτυο, χρησιμοποιεί ήδη κάποιο router τότε συμφέρει να αγοράσει το κατάλληλο επιπρόσθετο λογισμικό καθώς διατηρεί κατά αυτόν τον τρόπο χαμηλό το κόστος αναβάθμισης. Η αναβάθμιση του δρομολογητή δεν μπορεί να εγγυηθεί την ομαλή λειτουργία του εικονικού δικτύου καθώς στο μέλλον μπορεί να εμφανιστεί κάποια επιπλοκή κατά τη λειτουργία του router και το λογισμικό κρυπτογράφησης από μόνο του δεν θα μπορέσει να αποτρέψει μια πιθανή κατάρρευση του Εικονικού Ιδιωτικού Δικτύου. Στην παρακάτω εικόνα απεικονίζεται μία αρχιτεκτονική ενός vpn, βασίσμένη στον δρομολογητή (router). [25]



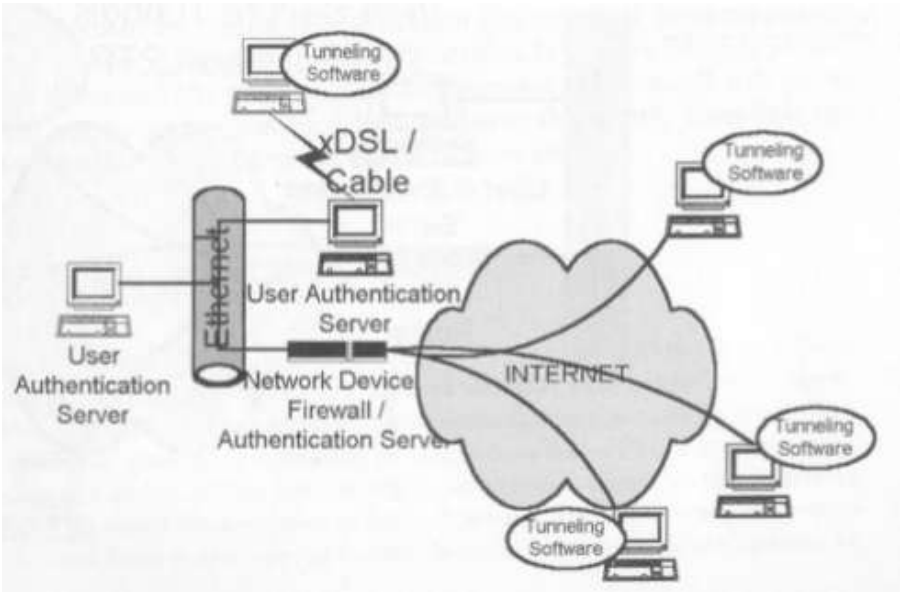
Εικόνα 12: Αρχιτεκτονική VPN που βασίζεται στον δρομολογητή.

3.2.5 VPNs που βασίζονται στην απομακρυσμένη σύνδεση (Remote Access)

Τα VPN αυτού του τύπου επεκτείνουν ένα δίκτυο και δίνουν τη δυνατότητα στους χρήστες να συνδέονται στο δίκτυο αυτό μέσω του VPN από οποιοδήποτε σημείο. Χρησιμοποιούνται από εταιρίες, ώστε να δίνουν δυνατότητα στους εργαζόμενους να συνδεθούν στα intranets και extranets των συνεργατών τους όποτε και από όπου αυτοί θέλουν. Η πρόσβαση σε αυτού του είδους τα VPNs είναι σχετικά εύκολη, καθώς μπορεί να γίνει για παράδειγμα μέσω μιας γραμμής ISDN ή ADSL. Σημαντικό είναι το γεγονός ότι ο αναγκαίος εξοπλισμός υλοποίησης του VPN δεν απαιτεί μεγάλη δαπάνη. Το ίδιο σημαντική είναι η ευκολία ανάπτυξης του δικτύου και η σύνδεση νέων χρηστών.

Κατά την υλοποίηση ενός VPN σημασία έχει από ποιον ξεκινάει η διαδικασία του τούνελ και της κρυπτογράφησης: από τον πελάτη (client) ή από τον εξυπηρετητή (server) πρόσβασης (Network Access Server – NAS). Στην περίπτωση που έχουμε έναρξη σύνδεσης από τον client, το κρυπτογραφημένο τούνελ εγκαθίσταται στον client χρησιμοποιώντας είτε το πρωτόκολλο IPSec, είτε το Layer 2 tunneling protocol (L2TP), είτε το Point-to-Point Tunneling Protocol (PPTP) καθιστώντας το δίκτυο του παροχέα υπηρεσιών απλά ένα μέσο μεταφοράς.

Η χρήστη των Εικονικών Ιδιωτικών Δικτύων (VPN) απομακρυσμένης πρόσβασης μείωσε σημαντικά το κόστος απομακρυσμένης σύνδεσης. Ο απομακρυσμένος χρήστης (Remote User) μπορεί να συνδεθεί με τον προσωπικό του υπολογιστή με κάποιο άλλο τοπικό δίκτυο (LAN) που βρίσκεται σε κάποιο άλλο γεωγραφικό σημείο μέσω του Διαδικτύου. Στην περίπτωη των VPNs απομακρυσμένης πρόσβασης, ο χρήστης πρέπει να διαθέτει κατάλληλο λογισμικό στον προσωπικό του υπολογιστή, προκειμένου να είναι σε θέση να ξεκινήσει τη διαδικασία tunneling και να έχει πρόσβαση σε ένα απομακρυσμένο δίκτυο. Το tunnel μπορεί να προέρχεται και από μια σύνδεση ISDN, ή VDSL ή κάποια άλλη. Η παρακάτω εικόνα απεικονίζει μια αρχιτεκτονική VPN απομακρυσμένης πρόσβασης. [25]



Εικόνα 13: Αρχιτεκτονική VPN απομακρυσμένης πρόσβασης.

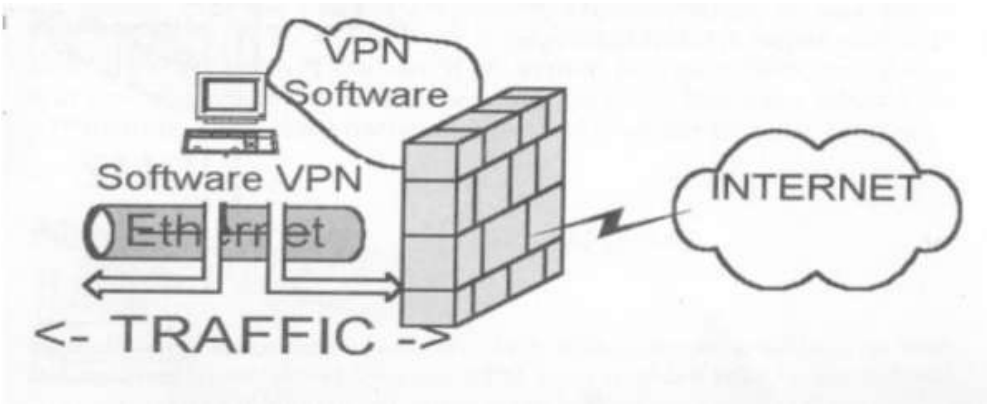
3.2.6 VPNs που βασίζονται στο λογισμικό (Software-based)

Βασική λειτουργία του λογισμικού στο οποίο βασίζεται το Εικονικό Ιδιωτικό Δίκτυο είναι να **δημιουργεί** κάποιο **tunnel** με έναν υπολογιστή (host) από την άλλη μεριά της σύνδεσης, παρέχοντας ταυτόχρονα την απαραίτητη κρυπτογράφηση των μεταδιδόμενων πακέτων**.** Κατά τη δημιουργία των tunnels επιτυγχάνεται η επικοινωνία μεταξύ των λογισμικών του πελάτη (client) και του εξυπηρετητή (Server) σύμφωνα με κάποιο πρωτόκολλο, όπως είναι το Point-to-Point Tunneling Protocol (PPTP).

Κατά την σύνδεση ενός υπολογιστή (host) με τον εξυπηρετητή (server) μιας επιχείρησης η πληροφορία κρυπτογραφείται, υφίσταται ενθυλάκωση και δρομολογείται προς τον παραλήπτη. Όταν ένα πακέτο δεδομένων φτάσει στον εξυπηρετητή (server), αυτός πιστοποιεί την ταυτότητα του χρήστη και αποκρυπρογραφεί τα δεδομένα με τον κατάλληλο αλγόριθμο, ώστε να πραγματοποιηθεί η μετάδοση της πληροφορίας με ασφάλεια μέσω του VPN.

Τα VPNs που βασίζονται στο λογισμικό (Software-based) παρέχουν τις λιγότερες υπηρεσίες σχετικά με τις υπόλοιπες αρχιτεκτονικές VPN και προτιμούνται για υπολογιστικά συστήματα μικρής ισχύος, τα οποία δεν υποστηρίξουν μεγάλο όγκο δεδομένων. Τα συγκεκριμένα εικονικά ιδιωτικά δίκτυα

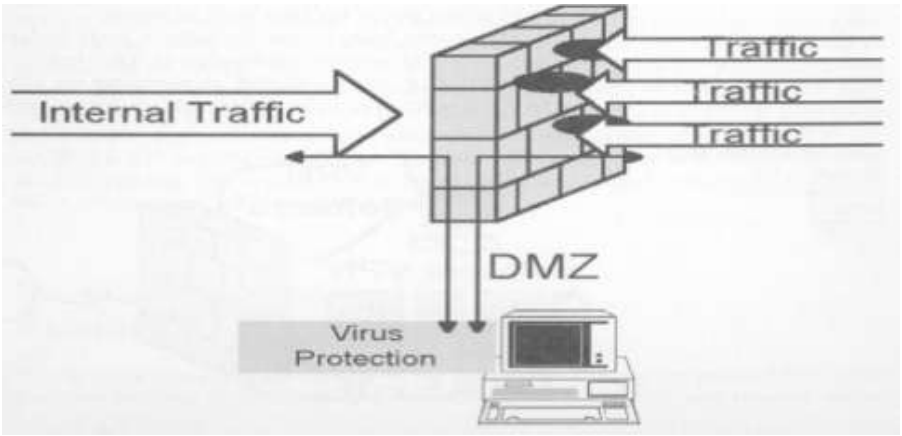
είναι κατάλληλα για συνδέσεις τύπου client-to-LAN. Η παρακάτω εικόνα απεικονίζει μια αρχιτεκτονική VPN Software-based. [25]



Εικόνα 14: Αρχιτεκτονική VPN Software-based.

3.2.7 VPNs που βασίζονται στις εφαρμογές multiservice και τα tunnel switching

Κύριος σκοπός των VPNs που βασίζονται στις εφαρμογές multiservice είναι η προστασία του δικτύου από τους συνεχώς αυξανόμενους και πιο επικίνδυνους ιούς. Επεξεργάζονται και φιλτράρουν κάθε είδους πληροφορία που προέρχεται από το Διαδίκτυο. Η συγκεκριμένη αρχιτεκτονική VPN δεν αποτελεί μια εντελώς καινούρια αρχιτεκτονική, αλλά πρόκειται για μια αναβαθμισμένη μορφή των ήδη υπαρχόντων firewall-based εικονικών δικτύων. Όλες οι πληροφορίες που εισέρχονται από το δημόσιο δίκτυο προς το ενδο-επιχειρησιακό δίκτυο αποκρυπτογραφούνται και αναλύονται πρώτα από το «αντιβιοτικό» πρόγραμμα **(antivirus)** που είναι ενσωματωμένο πάνω στο firewall του δικτύου. Στη συνέχεια, εφόσον η πληροφορία ελεγχθεί για ιούς και δεν περιλαμβάνει κακόβουλο τμήμα, μπορεί πλέον να διαπεράσει το ενδο-επιχειρησιακό δίκτυο. [25]



Εικόνα 15: Αρχιτεκτονική VPN multiservice application

3.2.8 VPNs που βασίζονται στο tunnel switching

Η αρχιτεκτονική Tunnel Switching σχεδιάστηκε με σκοπό να συνδυάσει τα χαρακτηριστικά και τις λειτουργίες όλων των προηγουμένων αρχιτεκτονικών, όπως για παράδειγμα τη δρομολόγηση των πακέτων ή του firewall, πάνω σε μια και μοναδική συσκευή δικτύου. Το νέο αυτό μοντέλο VPN είναι κατασκευασμένο ώστε να μπορεί να εξυπηρετήσει χιλιάδες απομακρυσμένους χρήστες, ενώ οι μηχανισμοί κρυπτογράφησης και ενθυλάκωσης είναι σχεδιασμένοι ώστε να μπορούν διαχειριστούν μια μεγάλη γκάμα πρωτοκόλλων δικτύου εκτός από το IP πρωτόκολλο. [25]

3.3 Διάκριση VPN με βάση τα πρωτόκολλα που χρησιμοποιούνται για την υλοποίηση τους

Αν η **διάκριση** γίνει με αντιστοίχιση του **VPN** με τα **επίπεδα OSI** στο οποίο λειτουργεί τότε διακρίνονται σε VPN **δευτέρου, τρίτου και τετάρτου επιπέδου**.

Σαν δευτέρου επιπέδου VPN θεωρούνται οι ATM και Frame Relay που είναι μηχανισμοί μεταγωγής πακέττων και έχουν πλέον κυρίως ιστορική σημασία.

Τα Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), Multi-Protocol Label Switching (MPLS) και IP Security (IPSec) είναι παραδείγματα τρίτου επιπέδου VPN.

Generic Routing Encapsulation (GRE) είναι ένα πρωτόκολλο που υλοποιεί και προσφέρει tunnels (κανάλια) για να μεταφέρει πακέτα μεταξύ δύο σημείων και έχει αναπτυχθεί από την Cisco Systems. Είναι κι αυτό ένα πρωτόκολλο δευτέρου επιπέδου που μπορεί να χρησιμοποιηθεί πάνω από IP. Μπορεί να ενφυλακώσει οποιαδήποτε πρωτόκολλα της IP στοίβας.

Layer 2 Tunneling Protocol (L2TP) είναι ένα πρωτόκολλο που υλοποιεί και προσφέρει tunnels (κανάλια) για να μεταφέρει πακέτα PPP μεταξύ δύο σημείων. Είναι στην ουσία ένα πρωτόκολλο δευτέρου επιπέδου που μπορεί να χρησιμοποιηθεί πάνω από το IP/UDP. Μπορεί να προσφέρει την tunneling υπηρεσία στο IP ή στο IPsec εφόσον απαιτείται ασφάλεια και ιδιωτικότητα.

Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την **ασφαλή μετάδοση και ανταλλαγή δεδομένων** (packets) **μέσω του στρώματος IP**. Το IPsec αποτελεί ένα από τους πιο διαδεδομένους τρόπους υλοποίησης VPNs και θα εξεταστεί με λεπτομέρια στη συνέχεια.

Οι τεχνολογίες τετάρτου επιπέδου SSL και TLS.

Από τις παραπάνω τεχνολογίες επιλέγουμε τις τεχνολογίες MPLS, IPsec και SSL σαν τις περισσότερο δημοφιλής για την υλοποίηση VPNs.

3.3.1 VPNs που βασίζονται στην τεχνολογία MPLS

Τα MPLS εικονικά ιδιωτικά δίκτυα είναι 3^{ου} επιπέδου και έχουν την δυνατότητα παροχής πολλαπλών υπηρεσιών στους χρήστες. Αρχικά, μπορούμε να αναφέρουμε τις μη προσανατολισμένες στη σύνδεση υπηρεσίες (Connectionless Service). Ένα πλεονέκτημα των MPLS VPNs είναι ότι ότι δεν χρειάζεται εκ των προτέρων εγκατάσταση καναλιού επικοινωνίας ανάμεσα στον αποστολέα και τον παραλήπτη. Είναι δηλαδή ενά «ασυνδεσιμκό» πρωτόκολλο. Η λειτουργία αυτή είναι ταυτόσιμη με τον τρόπο λειτουργίας του ίδιου του internet, το οποίο βασίζεται στο

πρωτόκολλο TCP/IP. Με τον τρόπο αυτό αποφεύγεται επιπλέον πολυπλοκότητα στη λειτουργία του δικτύου.

Τα VPNs δίνουν την δυνατότητα στους παροχείς υπηρεσιών να παρέχουν αρκετές υπηρεσίες σε ομάδες χρηστών. Η λειτουργία αυτή γίνεται μέσω της υπηρεσίας του Κεντρικού Ελέγχου (Centralized Service). Οι χρήστες μπορούν να χρησιμοποιούν αυτές τις υπηρεσίες μέσα στα δικά τους intranets και extranets.

Το πρωτόκολλο του MPLS στα εικονικά δίκτυα, δίνει τη Δυνατότητα αναβάθμισης (Scalability), εξαιτίας του ότι είναι ένα «ασυνδεσμικό» πρωτόκολλο, σε αντίθεση με άλλα είδη των VPNs (Frame Relay, ATM κλπ.), που χρησιμοποιούν προσανατολισμένες στην σύνδεση υπηρεσίες. Τα MPLS χρησιμοποιούν το λεγόμενο “peer” μοντέλο για να πετύχουν αυτή την αναβάθμιση. Αυτό σημαίνει ότι ο ένας χρήστης το μόνο που χρειάζεται είναι να συνδεθεί (peer) με το δρομολογητή του παροχέα (provider edge – PE – router) και όχι με όλους τους υπόλοιπους δρομολογητές που είναι μέλη του VPN. Δεν απαιτείται δηλαδή η δημιουργία κρυπτογραφικών tunnels ή μόνιμων εικονικών κυκλωμάτων VCs.

Τα εικονικά ιδιωτικά δίκτυα βασισμένα στο πρωτόκολλο του MPLS προσφέρουν το ίδιο επίπεδο ασφάλειας (Security) με τα προσανατολισμένα στην σύνδεση VPNs. Αυτό σημαίνει ότι δεδομένα ενός συγκεκριμένου VPN δεν μπορούν να βρεθούν σε ένα άλλο VPN. Η ασφάλεια παρέχεται τόσο από την πλευρά του παροχέα, ο οποίος εξασφαλίζει τα πακέτα ενός χρήστη να δρομολογούνται στο σωστό VPN, όσο και από το δίκτυο κορμού (backbone) του παροχέα, όπου η κυκλοφορία των VPN πακέτων γίνεται ξεχωριστά από άλλα πακέτα.

Επίσης, η Ευέλικτη διευθυνσιοδότηση (Flexible Addressing) που παρέχει το πρωτόκολλο MPLS στα εικονικά ιδιωτικά δίκτυα, βοηθάει ώστα να αυξηθεί η προσπελασιμότητα ενός VPN. Δηλαδή οι χρήστες έχουν τη δυνατότητα να σχεδιάσουν το δίκτυό τους ορίζοντας τις δικές τους ip διευθύνσεις, ανεξάρτητα από άλλους πελάτες του ίδιου παροχέα (ακόμα δηλαδή και αν κάποια ip διεύθυνση χρησιμοποιείται και από κάποιο άλλο χρήστη). Τα MPLS εικονικά δίκτυα, επιτρέπουν στους πελάτες να συνεχίσουν να χρησιμοποιούν τον δικό τους χώρο διευθύνσεων, χωρίς να γίνει μετάφραση αυτών (Network Address Translation – NAT), παρέχοντας έτσι μια δημόσια και μια ιδιωτική προβολή των διευθύνσεων. Μετάφραση γίνεται μόνον όταν δύο VPNs με επικαλυπτόμενες διευθύνσεις θέλουν να επικοινωνήσουν. Συνοψίζοντας, στα MPLS VPNs οι χρήστες χρησιμοποιούν τις δικές τους ιδιωτικές διευθύνσεις και επικοινωνούν ελεύθερα πάνω από τα δημόσια IP δίκτυα.

Μια άλλη υπηρεσία του MPLS εικονικού ιδιωτικού δικτύου είναι η Υποστήριξη κλάσεων υπηρεσιών (Class of service – CoS – support). Η CoS είναι μια υπηρεσία που προβλέπει την απόδοση και πολιτική υλοποίησης του εκάστοτε VPN, αλλά υποστηρίζει και τις υπηρεσίες πολλαπλών επιπέδων στα MPLS VPNs. Η άμεση εξάπλωση (Straightforward migration) των MPLS VPNs, αναφέρεται στη δυνατότητα του MPLS να μπορεί να εφαρμοστεί πάνω σε πολλές και διαφορετικές αρχιτεκτονικές δικτύων όπως IP, Frame Relay, ATM κλπ. Η εξάπλωση μέχρι τον τελικό χρήστη είναι απλή γιατί δεν είναι απαραίτητο να γίνει κάποια αλλαγή ούτε στον δρομολογητή CE του πελάτη, ούτε στο intranet που δουλεύει ώστε να υποστηρίξουν το MPLS.

Τα **πλεονεκτήματα χρήσης των MPLS** εικονικών ιδιωτικών δικτύων είναι αρκετά. Αρχικά, η μειώνουν το κόστος ενός VPN. Δηλαδή παρέχουν εναν οικονομικό τρόπο σύνδεσης των γραφείων

μιας εταιρίας ή οργανισμού, των τηλεπικοινωνιακών συσκευών και των κινητών χρηστών μέσα σε ένα intranet που λειτουργεί πάνω από μία δημόσια υποδομή του internet.

Επίσης, τα MPLS εικονικά ιδιωτικά δίκτυα, έχουν τη δυνατότητα εύκολης αναβάθμισης, καθώς είναι μη προσανατολισμένα στη σύνδεση, σε αντίθεση με άλλα είδη δικτύων VPNs, όπως τα IPSec, Layer 2 tunneling protocol (L2TP), Layer 2 forwarding protocol (L2FP), Generic routing encapsulation (GRE), Frame relay, ATM protocols, τα οποία αναβαθμίζονται πιο δύσκολα. Αυτό συμβαίνει διότι βασίζονται σε πλήρεις τοπολογίες από κρυπτογραφικά tunnels ή από μόνιμα εικονικά κυκλώματα, γεγονός το οποίο καθιστά την προσθήκη νέων πελατών περισσότερο δύσκολη. Είναι λοιπόν πιο εύκολο να δημιουργηθούν και να διαχειριστούν απ' ότι τα συμβατικά εικονικά ιδωτικά δίκτυα. Επιπλέον, κάθε MPLS VPN μπορεί να παρέχει προστιθέμενης αξίας υπηρεσίες, όπως φύλαξη δεδομένων και εφαρμογών, δίκτυα επιχειρήσεων και τηλεφωνικές υπηρεσίες.

Συνοψίζοντας, τα MPLS VPNs προσφέρουν:

- Μία πλατφόρμα για την ταχύτατη ανάπτυξη προστιθέμενης αξίας IP υπηρεσιών όπως intranets, extranets, φωνή, πολυμέσα και δικτυακές επιχειρήσεις.
- Ιδιωτικότητα και ασφάλεια αντίστοιχη των Layer-2 VPNs, περιορίζοντας τις VPN διαδρομές μόνο ανάμεσα σε εκείνους τους δρομολογητές που είναι μέλη του VPN.
- Ενσωμάτωση των intranets των πελατών, χωρίς καμία περικοπή.
- Αυξημένη δυνατότητα αναβάθμισης, έτσι ώστε να μπορούν να φιλοξενηθούν χιλιάδες sites ανά VPN και δεκάδες ή και χιλιάδες VPN ανά παροχέα.
- IP – Class of Service (CoS), υποστήριξη πολλών κλάσεων υπηρεσιών και προτεραιοτήτων εντός του VPN ή ανάμεσα στα VPNs.
- Εύκολη διαχείριση των μελών ενός VPN.
- Κλιμακωτή διασύνδεση εξωτερικών intranets και extranets που περικλείουν πολλές επιχειρήσεις. [27]

3.3.2 VPNs που βασίζονται στο πρωτόκολλο IPSec

Προκειμένου να διασφαλιστεί η ασφαλής μετάδοση δεδομένων μέσω ενός δικτύου IP, δημιουργήθηκε ένα νέο πρωτόκολλο με μηχανισμούς κρυπτογράφησης, το οποίο είναι εφαρμόσιμο σε IP δίκτυα. Η ανάγκη για τη δημιουργία ενός τέτοιου πρωτοκόλλου προέκευψε από το γεγονός ότι τα πρωτόκολλα TCP/IP δεν παρέχουν μηχανισμούς κρυπτογράφησης. Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την **ασφαλή μετάδοση και ανταλλαγή δεδομένων** (packets) **μέσω του στρώματος IP**. Το IPSec σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN. Ως προς τα επίπεδα του OSI, **αντιστοιχίζεται στο επίπεδο 3 (επίπεδο δικτύου).**

Γεγονός αποτελεί, ότι με τη χρησιμοποίηση του Διαδικτύου για τη πραγματοποίηση επικοινωνιών μέσα από εικονικά δίκτυα, ανακύπτουν διάφορα θέματα ασφάλειας. Αρχικά μπορεί να αναφερθεί η **Απώλεια της Ιδιωτικότητας των Δεδομένων** (Loss of Privacy), όπου ένας μη εξουσιοδοτημένος χρήστης, ο οποίος έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο, έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνησή τους από το ένα άκρο στο άλλο μέσω του Διαδυκτόυ (Internet).

Ένα δεύτερο ζήτημα είναι η **Απώλεια Ακεραιότητας Δεδομένων** (Loss of Data Integrity), όπου ένας μη εξουσιοδοτημένος χρήστης τροποποιεί τα δεδομένα που μεταφέρονται στο δίκτυο, όπως για παράδειγμα τους αριθμούς ενός λογαριασμού καταθέσεων.

Επίσης, η **Προσποίηση Ταυτότητας** (Identity Spoofing) αναφέρεται σε ένα μη εξουσιοδοτημένος χρήστης, ο οποίος παριστάνει ότι είναι ένας νόμιμος χρήστης του δικτύου και ζητά πληροφορίες που σε διαφορετική περίπτωση δε θα μπορούσε να έχει. Τέλος, ένα ζήτημα ασφαλεία που μπορεί να προκύψει είναι η **Άρνηση Υπηρεσιών** (Denial-of-Service), σύμφωνα με την οποία γίνεται "επίθεση" σε κάποιον server του δικτύου.

Η αντιμετώπιση των παραπάνω απειλών είναι βασικό μέλημα του Ο βασικός λοιπόν στόχος του πρωτοκόλλου IPSec, χωρίς να απαιτείται πρόσθετος εξοπλισμός, ούτε να υπάρχει ανάγκη για ένα σύνολο τροποποιήσεων και αλλαγών σε διάφορες εφαρμογές.

Η **Ακεραιότητα των δεδομένων** (Integrity), σύμφωνα με την οποία διασφαλίζεται η ακέραια μεταφορά των πακέτων από το ένα άκρο στο άλλο (αποστολέας – παραλλήπτης), αποτελεί μια υπηρεσία που προσφέρει το πρωτόκολλο IPSec. Δηλασή η συγκεκριμένη υπηρεσία διασφαλίζει ότι τα πακέτα των δεδομένων κατά την διάρκεια της μεταφοράς τους δεν θα αλλοιωθούν ή παραποιηθούν, από «εισβολείς» ή από τυχόν σφάλματα επικοινωνίας.

Μια δεύτερη υπηρεσία που προσφέρει το πρωτόκολλο IPSec, είναι η **Εξακρίβωση γνησιότητας της προέλευσης των δεδομένων** (Authentication) ή πιστοποίηση ταυτότητας, που επαληθεύει ότι τα δεδομένα στάλθηκαν πράγματι από το χρήστη που ισχυρίζεται ότι τα έστειλε.

Μια ακόμη υπηρεσία, αποτελεί η **Εμπιστευτικότητα** (Confidentiality), που προσφέρει τη δυνατότητα αναγνώρισης και επεξεργασίας των δεδομένων μόνο από εγκεκριμένους χρήστες.

Το IPSec αναφέρεται σε δύο διαφορετικά είδη πρωτοκόλλων (όπως ορίζεται στα RFC 2401-2411 και RFC 2451), δηλαδή τα πρωτόκολλα **σχετικά με την ασφάλεια** και τα πρωτόκολλα **σχετικά με την ανταλλαγή κλειδιών**. Η πρώτη κατηγορία αναφέρεται σε πρωτόκολλα τα οποία καθορίζουν αφενός τον τρόπο με τον οποίο θα γίνει η κρυπτογράφηση των δεδομένων και αφετέρου την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι εμπιστευτικότητας, ακεραιότητας και πιστοποίησης ταυτότητας. Η δεύτερη κατηγορία αναφέρεται σε ένα άλλο είδος ασφάλειας μεταξύ αποστολέα και παραπήπτη. Δηλαδή καθορίζει ένα προκαθορισμένο «κλειδί» που θα γνωρίζουν μόνο αυτοί κατά την επικοινωνία τους, ώστε τα δεδομένα να ανταλάσσονται μεταξύ τους με ασφάλεια.

Προκειμένου λοιπόν το πρωτόκολλο IPSec να διασφαλίσει τις απαιτήσεις ασφαλείας που περιεγράφηκαν παραπάνω, ορίζεται ένα νέο σετ κεφαλίδων το οποίο προστίθεται σε κάθε IP πακέτο. Προκύπτουν έτσι καινούρια IP πακέτα τα οποία είναι μεγαλύτερα σε μέγεθος από τα αρχικά και έχουν διαφορετική δομή. Αυτές οι νέες κεφαλίδες που διασφαλίζουν την ασφάλεια των IP πακέτων μπορεί να αναφέρονται είτε στην **κεφαλίδα πιστοποίησης ταυτότητας** (AH — Authentication Header), είτε στην κεφαλίδα για **Ασφαλή Ενθυλάκωση της πληροφορίας.**

Η κεφαλίδα **πιστοποίησης ταυτότητας** διασφαλίζει την ακεραιότητα, την πιστοποίηση ταυτότητας των δεδομένων, καθώς και την αποφυγή δημιουργίας και αποστολής ίδιων πακέτων. Η κεφαλίδα πιστοποίησης ταυτότητας, δεν παρέχει ασφάλεια εμπιστευτικότητας. Η ακεραιότητα και η πιστοποίηση των δεδομένων πραγματοποιούνται τόσο από τον αποστολέα, όσο και από τον

παραλήπτη που βρίσκονται στα άκρα του tunnel, εκτελώντας μία συνάρτηση κατακερματισμού στο IP πακέτο. Χρησιμοποιούν δηλαδή ένα κοινό κλειδί (Message Authentication Code – MAC) μεταξύ τους. Αυτή η συνάρτηση κατακερματισμού όταν εφαρμοστεί έχει ένα αποτέλεσμα που δεν κρυπτογραφείται και χρησιμοποιείται απλά από το άλλο άκρο της επικοινωνίας (αποστολέα ή παραλήπτη) για να ελέγξει ότι τα δεδομένα δεν έχουν τροποποιηθεί. Το γεγονός αυτό καθ' αυτό της χρησιμοποίησης ενός κοινού μυστικού κλειδιού που είναι γνωστό και στα δύο μέρη (αποστολέας-δέκτης) εγγυάται την πιστοποίηση της ταυτότητας των συμβαλλομένων.

Η κεφαλίδα για **Ασφαλή Ενθυλάκωση της πληροφορίας (Encapsulating Security Payload – ESP)** παρέχει υπηρεσίες για την πιστοποίηση και ακεραιότητα των πακέτων IP που διαβιβάζονται μεταξύ δύο άκρων. Επιπρόσθετα, παρέχει εμπιστευτικότητα μέσω μεθόδων κρυπτογράφησης. Η πιστοποίηση και η ακεραιότητα μπορούν να διασφαλιστούν με τον ίδιο τρόπο που τα παρέχει και η κεφαλίδα πιστοποίησης ταυτότητας. Το ESP παρέχει εμπιστευτικότητα μέσω της κρυπτογράφησης ενός IP πακέτου. Το ESP υποστηρίζει ένα μεγάλο αριθμό συμμετρικών αλγορίθμων κρυπτογράφησης. Η πιο συνηθισμένη επιλογή είναι ο αλγόριθμος **AES (128-bit).** Εκτός από τον αλγόριθμο αυτό υπάρχουν και μπορούν να χρησιμοποιηθούν άλλοι αλγόριθμοι – όπως για παράδειγμα ο 3DES ή ο απλός DES.

Συσχετίσεις Ασφάλειας

Το IPSec παρέχει πολλές επιλογές για την υλοποίηση κρυπτογράφησης και πιστοποίησης ταυτότητας στο δίκτυο. Κάθε IPSec σύνδεση μπορεί να παρέχει **είτε κρυπτογράφηση (με ESP)** είτε **ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων (με AH)** ή και **τα δύο**. Όταν η υπηρεσία ασφάλειας καθοριστεί, τα δύο άκρα επικοινωνίας, πρέπει να καθορίσουν ακριβώς ποιους αλγόριθμους θα χρησιμοποιήσουν (για παράδειγμα, **AES ή 3DES για κρυπτογράφηση** και **MD5 ή SHA για ακεραιότητα δεδομένων**)[1]. Αφού αποφασίσουν για τους αλγόριθμους οι δύο συσκευές πρέπει να **μοιράσουν κλειδιά σύνδεσης**. Η συσχέτιση ασφάλειας **(Security Association – SA)** είναι μια μέθοδος που χρησιμοποιείται από το IPSec για την παρακολούθηση όλων των λεπτομερειών που αφορούν μία δεδομένη IPSec επικοινωνία. Μια συσχέτιση ασφάλειας είναι η σχέση μεταξύ αποστολέα και παραλήπτη που περιγράφει τις παραμέτρους επικοινωνίας, όπως αλγόριθμοι κρυπτογράφησης και αυθεντικοποίησης, τρόπος ανταλλαγής κλειδιών, διάρκεια ισχύος τους κτλ.

Οι κύριες παράμετροι που προσδιορίζονται σε μία συσχέτιση ασφαλείας (SA) είναι η IP διεύθυνση πηγής και προορισμού, ένα ID χρήστη, το πρωτόκολλο μεταφοράς (TCP ή UDP), ο αλγόριθμος για έλεγχο πιστοποίησης ταυτότητας, καθώς και τα αντίστοιχα κλειδιά, ο αλγόριθμος που χρησιμοποιείται για κρυπτογράφηση, καθώς και τα αντίστοιχα κλειδιά, ο τρόπος λειτουργίας του IPSec (transfer ή tunnel mode) και η διάρκεια ζωής μιας συσχέτισης ασφαλείας (SA).

Πρωτόκολλο Διαχείρισης Κλειδιών - IKE (Internet Key Exchange)

Το IPSec περιλαμβάνει το πρωτόκολλο ανταλλαγής κλειδιού IKE (Internet Key Exchange), προκειμένου να καθορίσει τον τρόπο ρύθμισης των συσχετίσεων ασφάλειας. Το πρωτόκολλο IKE δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι (tunnel) μεταξύ των δύο άκρων (αποστολέα και παραλήπτη) και διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec. Αυτή η διαδικασία

[1] Οι MD5 και SHA είναι αλγόριθμοι που χρησιμοποιεί το πρωτόκολλο IPSec, προκειμένου να διασφαλίσει την ακεραιότητα των δεδομένων.

απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν συγκεκριμένα κλειδιά μεταξύ τους. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί:

- Προ-Μοιρασμένα Κλειδιά—Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας συνάρτησης κατακερματισμο) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.
- Κρυπτογράφηση Δημοσίων Κλειδιών—Κάθε μηχανή παράγει έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το δημόσιο κλειδί (public key) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού, αποκρυπτογραφώντας με τα ιδιωτικά κλειδιά (private keys) ό,τι λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.
- Ψηφιακές Υπογραφές—Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Ο αποστολέας χρησιμοποιεί το κρυφό του ιδιωτικό κλειδί για να υπογράψει ηλεκτρονικά τα δεδομένα του. Ο αποδέκτης του κειμένου χρησιμοποιεί το public key του αποστολέα, το οποίο έτσι και αλλιώς γνωρίζει αφού είναι δημόσιο, για να ελέγξει την υπογραφή του αποστολέα. Αν αυτός ο έλεγχος είναι επιτυχής, αυτό σημαίνει ότι το κείμενο δεν έχει αλλαχθεί και έχει πιστοποιηθεί η ταυτότητα του αποστολέα Υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Μετά την πιστοποίηση της ταυτότητας του κάθε χρήστη, πρέπει να υπάρξει η ανταλλαγή του κλειδιού που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων που θα σταλούν κατά την επικοινωνία των δύο χρηστών. Ως βασικό αλγόριθμο ανταλλαγής κλειδιού το IKE υποστηρίζει τον Diffie-Hellman, αν και μπορεί να υπάρξουν και άλλοι.

Τα βήματα που ακολουθεί ο αγόριθμος IPSec σε μια επικοινωνία ανταλλαγής δεδομένων μεταξύ δύο άκρων με τη χρήση του είναι τα ακόλουθα:

1. Ενεργοποίηση μιας IPSec επικοινωνίας. Στο βήμα αυτό καθορίζεται το σύνολο των IP πακέτων που πρόκειται να προστατευθούν μέσω του πρωτοκόλλου IPSec.
2. IKE – Πρώτη φάση. Δημιουργία και λειτουργία της IKE Συσχέτισης Ασφαλείας.
3. IKE – Δεύτερη φάση. Δημιουργία και λειτουργία της AH/ESP Συσχέτισης Ασφαλείας
4. Μεταφορά Δεδομένων. Τα IP πακέτα που επιλέχθηκαν από το πρώτο βήμα μεταφέρονται.
5. Τερματισμός της IPSec επικοινωνίας. Εφόσον ολοκληρωθεί η μεταφορά των IP πακέτων, η IPSec επικοινωνία τερματίζεται. [3]

3.3.3 VPNs που βασίζονται στο πρωτόκολλο SSL

Η εταιρία Netscape Communications Corporation ανέπτυξε το πρωτόκολλο SSL (Secure Socket Layer) προκειμένου να διασφαλίσει την ασφαλή ανταλλαγή ευαίσθητων πληροφοριών, όπως οι αριθμοί πιστωτικών καρτών. Τον Ιούλιο του 1994 κυκλοφόρησε η πρώτη έκδοση (version 1.0)

του πρωτοκόλλου, ενώ το Δεκέμβριο του 1994 εκδίδεται μια αναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Η τρίτη έκδοση του SSL (version v.3.0) τέθηκε επισήμως σε κυκλοφορία το Δεκέμβριο του 1995 και πραματοποιήθηκε με δημόσια αναθεώρηση και σημαντική συνεισφορά από τη βιομηχανία. Μετεξελίχτηκε στο TLS (Transport Layer Security). Κύριο χαρακτηριστικό του πρωτοκόλλου αυτού είναι ότι παρέχει TCP/IP ασφάλεια μεταξύ δύο συστημάτων, όπου το ένα δρα σαν πελάτης (client) και το άλλο σαν εξυπηρετητής (server).

Το πρωτόκολλο SSL είναι ήδη εγκατεστημένο σε οποιοδήποτε Η/Υ που είναι συνδεδεμένος στο Διαδίκτυο και χρησιμοποιεί ένα πρόγραμμα περιήγησης (browser) χωρίς κάποια ιδιαίτερη ρύθμιση. Το πρωτόκολλο SSL είναι ανεξάρτητο από το λειτουργικό σύστημα του εκάστοτε υπολογιστή και επιτρέπει την κλιμάκωση στον έλεγχο πρόσβασης σε διάφορες εφαρμογές.

Έχει τη δυνατότητα να ελέγξει την πρόσβαση σε extranet VPNs ή VPNs απομακρυσμένης πρόσβασης. Ο χρήστης, μέσω ενός SSL VPN, έχει πρόσβαση σε εφαρμογές Web από οποιοδήποτε σημείο βρίσκεται με την απλή χρήση ενός προγράμματος πειήγησης (Web browser), μίας σύνδεσης στο Internet και χωρίς την ανάγκη ύπαρξης κάποιου ιδιαίτερου λογισμικού στον υπολογιστή του. Τα SSL VPNs μπορούν να «περάσουν» πάνω από firewalls και να αντιμετωπίσουν θέματα NAT (Network Address Translation).

Το πρωτόκολλο SSL διασφαλίζει την ασφαλή σύνδεση μεταξύ των δύο άκρων που επικοινωνούν μεταξύ του, μέσω της πιστοποίησης, της ταυτότητάς τους, καθώς και μέσω της κρυπτογράφησης των δεδομένων που ανταλλάσσονται.

Είναι ενσωματωμένο στην κορυφή μίας υπηρεσίας μεταφοράς δεδομένων, όπως εκείνη που παρέχεται από το πρωτόκολλο TCP/IP. Ένα σημαντικό πλεονέκτημα του πρωτοκόλλου SSL, είναι η η ανεξαρτησία του από την εκάστοτε εφαρμογή, που σημαίνει ότι μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια διαφανώς (transparently) σε οποιαδήποτε TCP/IP εφαρμογή.

Συνοπτικά, μπορεί να αναφερθεί ότι το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν Server (εξυπηρετητής) και το άλλο σαν client (εξυπηρετούμενος). Αυτή η ασφάλεια έχει τρεις βασικές ιδιότητες:

1. Γίνεται πιστοποίηση ταυτότητας και των δύο άκρων (αποστολέα – παραλήτη), μέσω κρυπτογράφισης ενός δημόσιου κλειδιού.
2. Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων μέσω κρυπτογράφησης.
3. Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων με χρήση των διευθύνσεων MAC των δύο άκρων.

Το πρωτόκολλο SSL συντονίζει τις συνθήκες σύνδεσης, τόσο του εξυπηρετούμενου (client), όσο και του εξυπηρετητή (server). Τα δύο άκρα που επικοινωνούν, μπορούν να έχουν πολλαπλές ταυτόχρονες συνδέσεις μεταξύ τους.

Τα δύο βασικά πρωτόκολλα που χρησιμοποιεί το SSL είναι το **SSL Record Protocol** και το **SSL Handshake Protocol**. Συνοπτικά, το SSL Record Protocol παρέχει υπηρεσίες εμπιστευτικότητας κα ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή των μηνυμάτων. Το SSL Handsake Protocol, ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών, το οποίο διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα

χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του Server και και του client όπου αυτό απαιτείται.

Μετά την ολοκλήρωση του SSL Handshake Protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας. Πιο συγκεκριμένα, το SSL Record Protocol λαμβάνει δεδομένα από πρωτόκολλα υψηλότερων επιπέδων και πραγματοποιεί κατακερματισμό (fragmentation), συμπίεση και κρυπτογράφηση δεδομένων. Κάθε ωφέλιμο φορτίο δεδομένων SSL Record Protocol μπορεί να συμπιέζεται και να κρυπτογραφείται σύμφωνα με την τρέχουσα μέθοδο συμπίεσης και τον αλγόριθμο κρυπτογράφησης.

Σκοπός του SSL Handshake Protocol είναι να ορίζει τα πρωτόκολλα που θα χρησιμοποιηθούν κατά τη διάρκεια της επικοινωνίας μεταξύ του πελάτη (client) και του εξυπηρετητή (server), να επιλέγουν τη μέθοδο συμπίεσης και την προδιαγραφή κρυπτογραφίας, να γίνεται αυθεντικοποίηση των δύο άκρων (server & client) και να δημιουργούν ένα κύριο μυστικό κλειδί (master secret key), από το οποίο προκύπτουν διάφορα κλειδιά για αυθεντικοποίηση και κρυπτογράφηση των μηνυμάτων.

Ένα μειονέκτημα του SSL είναι οι περιορισμένες εφαρμογές που μπορεί να εξυπηρετήσει. Επιπλέον, όλες αυτές οι εφαρμογές είναι απομακρυσμένης πρόσβασης μόνο (και όχι δίκτυο-προς-δίκτυο οι οποίες μπορούν να υποστηριχτούν από το IPSec). Θα λέγαμε λοιπόν ότι μεγάλη πληθώρα αναγκών που καλύπτει το IPSec δεν καλύπτονται από το SSL. Από την άλλη υπερτερεί ως προς το IPSec ως προς το κόστος αλλά και την πολυπλοκότητα υλοποίησης. [28]

ΚΕΦΑΛΑΙΟ 4: ΑΣΦΑΛΗΣ ΜΕΤΑΔΟΣΗ ΔΕΔΟΜΕΝΩΝ

4.1 Εισαγωγή

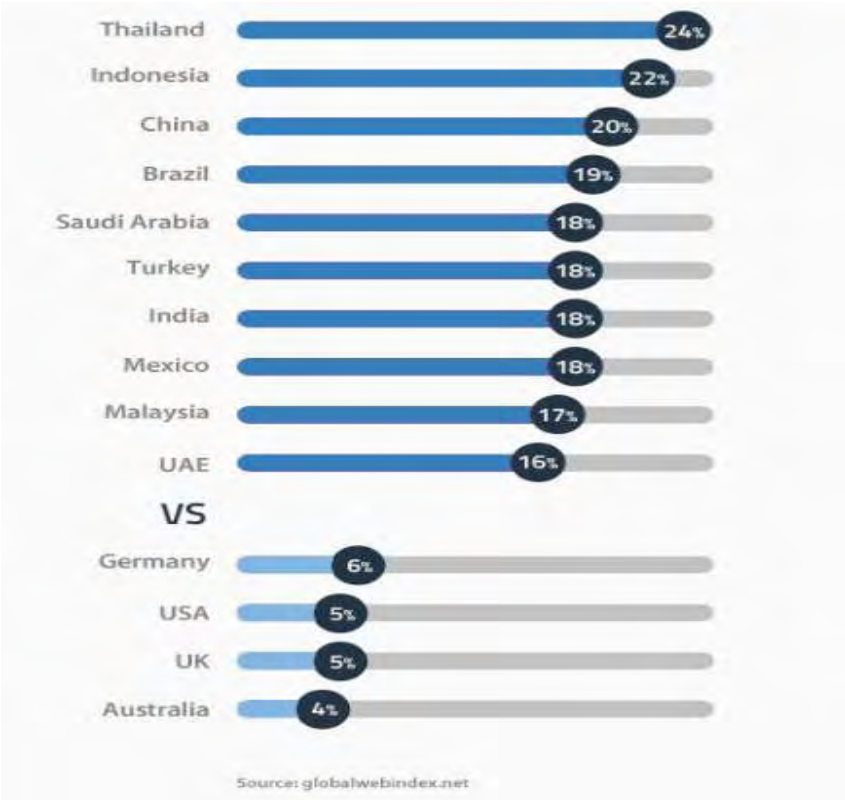
Αναμφισβήτητα, η αλματώδης πρόοδος της τεχνολογίας έχει χαρακτηρίσει τον αιώνα μας και έχει επιφέρει ριζικές αλλαγές στο σύγχρονο κόσμο. Παρά όμως τα πολλαπλά οφέλη της τεχνολογίας σε όλους τους τομείς, δεν είναι δυνατόν να υποτιμήσουμε και τις αρνητικές επιπτώσεις της, μια εκ των οποίων είναι η κατάργηση της ιδιωτικότητας και η ανεξέλεγκτη χρήση των προσωπικών δεδομένων.

Είναι γεγονός ότι οι κυβερνήσεις όλου του κόσμου νομοθετούν πλαίσια, που τους δίνουν τη δυνατότητα να παρακολουθούν, να αποθηκεύουν και να έχουν στη διάθεσή τους ανά πάσα στιγμή τα προσωπικά δεδομένα κάθε ατόμου. Δηλαδή, είναι σε θέση να γνωρίζουν κάθε τηλεφωνική επικοινωνία, μήνυμα ή email και κάθε ιστοσελίδα που επισκέπτεται ο χρήστης. Με τον τρόπο αυτό, μπορούν να έχουν στη διάθεσή τους λεπτομέρειες της καθημερινότητας και της προσωπικής ζωής των πολιτών.

Ένας ασφαλής τρόπος για τη διαφύλαξη των προσωπικών δεδομένων και την ιδιωτικότητά τους, είναι η χρήση της τεχνολογίας VPN. Τα VPNs δυσκολεύουν τους χάκερ, ή οποιονδήποτε τρίτο, να παρακολουθήσει τις επικοινωνίες και τις διαδικτυακές δραστηριότητες των χρηστών.

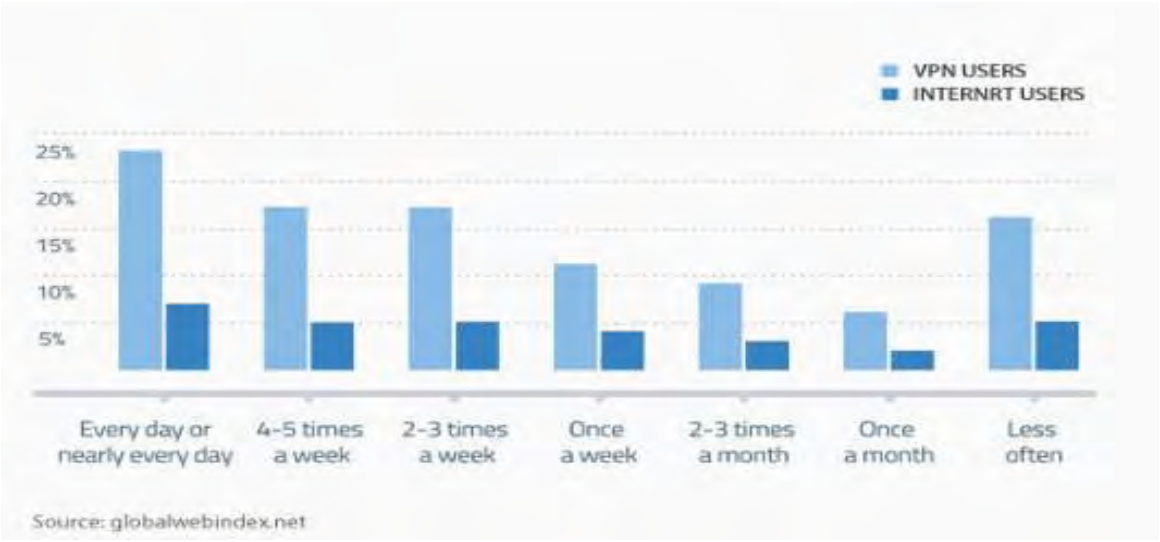
4.2 Στατιστικά στοιχεία χρήσης του VPN το έτος 2016

Σύμφωνα με την έρευνα του "globalwebindex.net" παρατηρούμε ότι η **Ασία** και η **Μέση Ανατολή** εξακολουθούν να **κυριαρχούν στην αγορά των VPNs**. Στην παρακάτω εικόνα παρουσιάζονται οι δέκα χώρες που συγκεντρώνουν τα μεγαλύτερα ποσοστά χρήσης του VPN.



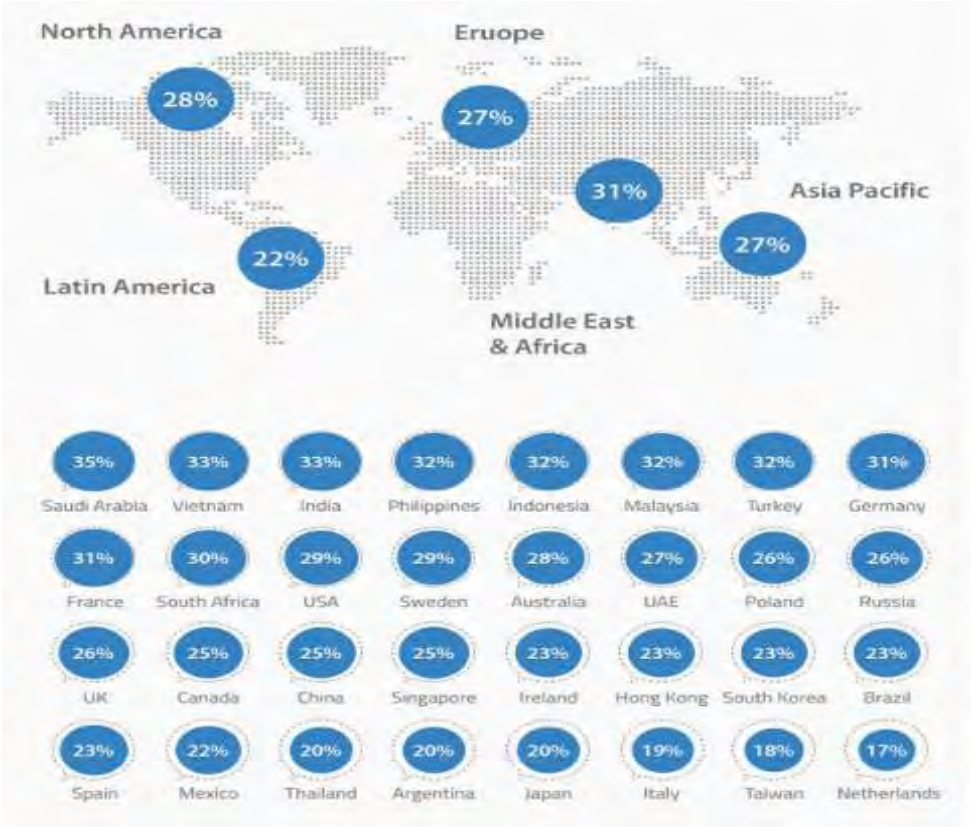
Εικόνα 16: 10 χώρες, τα μεγαλύτερα ποσοστά χρήσης του VPN.

Στην παρακάτω εικόνα, σύμφωνα με έρευνα που πραγματοποιήθηκε από την ίδια εταιρία, παρουσιάζονται **τα ποσοστά σχετικά με τη συχνότητα χρήσης του VPN**. Παρατηρούμε, ότι η πλειοψηφία των ανθρώπων που χρησιμοποιούν VPN, το χρησιμοποιούν **τουλάχιστον μια φορά την εβδομάδα.**



Εικόνα 17: Συχνότητα χρήσης του VPN.

Παρακάτω, ακολουθούν τα **ποσοστά των χρηστών ανά χώρα που χρησιμοποιούν την ανώνυμη περιήγηση στο διαδίκτυο**. Βλέπουμε ότι τα μεγαλύτερα ποσοστά συγκεντρώνουν η **Σαουδική Αραβία** με ποσοστό **35%,** η **Ινδία** και το **Βιετνάμ** με ποσοστό **33%.** Η ανώνυμη περιήγηση στο διαδίκτυο βασίζεται στη χρήση κάποιου VPN.



Εικόνα 18: Ποσοστά των χρηστών ανά χώρα που χρησιμοποιούν την ανώνυμη περιήγηση στο διαδίκτυο.

Τέλος, να αναφέρουμε ότι υπάρχουν διάφοροι λόγοι που η προστασία των προσωπικών δεδομένων συχνά αποτυγχάνει. Το γεγονός αυτό οφείλεται κατά κύριο λόγο με ποσοστό **93%** στην **εξέλιξη της τεχνολογίας** και τις δυνατότητες που προσφέρει. **Η μη ύπαρξη πολιτικών απορρήτου** κατέχει το μικρότερο ποσοστό με **24%**. Στο παρακάτω διάγραμμα απεικονίζονται οι λόγοι για τους οποίους αποτυγχάνει η προστασία των προσωπικών δεδομένων, καθώς και τα αντίστοιχα ποσοστά. Κατά 56% αποτυγχάνει λόγω ανεπαρκούς ενημέρωσης των εργαζομένων, κατά 45% λόγω έλλειψης κονδυλίων για αγορά και εφαρμογή τεχνολογικών λύσεων, κατά 36% λόγω έλλειψης διαδικασιών για την κατάρτιση των εργαζομένων και τον έλεγχο συμπεριφοράς τους, κατά 27% λόγω άγνοιας της νομοθεσίας. [29]

Εικόνα 19: Αιτίες σε ποσοστά μη ύπαρξης προσωπικών δεδομένων.

4.3 Κρυπτογράφηση

Η κρυπτογράφηση, δηλαδή η ασφαλής μετάδοση των δεδομένων χωρίς να δίνεται η δυνατότητα σε τρίτους να υποκλέψουν τα δεδομένα της επικοινωνίας, είναι ένα από τα κυριότερα θέματα που αφορούν τα VPNs. Για να πραγματοποιηθεί η κρυπτογράφηση, υπάρχει μια ευρεία γκάμα αλγορίθμων κρυπτογράφησης σχεδόν για όλα τα επίπεδα του OSI και ο χρήστης του VPN έχει την δυνατότητα να επιλέξει το επίπεδο ασφαλείας που επιθυμεί, σύμφωνα με τις εφαρμογές που

χρησιμοποιεί. Η ασφάλεια των VPNs βασίζεται στην κρυπτογραφική δυνατότητα των αλγορίθμων κρυπτογράφησης.

Το ένα σκέλος της διαδικασίας αποτελεί η κρυπτογράφηση, δηλαδή η μετατροπή ενός απλού κειμένου σε κρυπτογραφημένο κείμενο. Το άλλο σκέλος της διαδικασίας αποτελεί η αποκρυπτογράφηση, η ακριβώς αντίθετη διαδικασία, δηλαδή η μετατροπή της κρυπτογραφημένης πληροφορίας σε μη κρυπτογραφημένη. Με άλλα λόγια, όταν το κρυπτογραφημένο κείμενο φτάσει στον παραλήπτη, θα πρέπει να ακολουθηθεί η αντίστροφη διαδικασία και να γίνει η αποκρυπτογράφηση του μηνύματος. Το κρυπτογραφημένο μήνυμα δεν έχει κάποια σχέση με το αποκρυπτογραφημένο. Αυτά τα δύο κείμενα τα συνδέει μεταξύ τους μια σχέση, η οποία είναι το κλειδί της κρυπτογράφησης.

4.3.1 Private Key

Ο αποστολέας και ο παραλήπτης ενός μηνύματος χρησιμοποιούν κάποιους κοινούς χαρακτήρες στην αρχή, δηλαδή ένα κλειδί (private key), το οποίο γνωρίζουν μόνον οι ίδιοι. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να το αποκρυπτογραφήσει. Αυτή η μέθοδος κρυπτογραφίας ονομάζεται **«μυστικού κλειδιού» (secret key) ή συμμετρική κρυπτογραφία** και θεωρείται μία από τις πιο ασφαλείς μεθόδους. Σοβαρό πρόβλημα της μεθόδου αυτής αποτελεί ο τρόπος με τον οποίο ο αποστολέας και ο παραλήπτης θα συμφωνήσουν για το κλειδί και πώς θα το ανταλλάξουν μεταξύ τους.

Το πρόβλημα γίνεται πιο σοβαρό, όταν ο αποστολέας και ο παραλήπτης βρίσκονται σε διαφορετική γεωγραφική περιοχή. Στην περίπτωση αυτή, το θέμα είναι αν μπορούν να εμπιστευτούν είτε το δίκτυο, είτε το ταχυδρομείο είτε το τηλέφωνο. Αν και αυτή η μέθοδος θεωρείται αρκετά ασφαλής, είναι δύσκολο να εφαρμοσθεί σε δίκτυα VPN όπου οι διάφοροι hosts δεν βρίσκονται στην ίδια γεωγραφική περιοχή. Αν λάβουμε υπόψη ότι τα περισσότερα δίκτυα VPN συνδέουν υπολογιστές που απέχουν πολύ μεταξύ τους, καθόσον βρίσκονται σε διαφορετικές γεωγραφικές περιοχές, καταλήγουμε στο συμπέρασμα ότι η συγκεκριμένη μέθοδος εφαρμόζεται σε εξειδικευμένες περιπτώσεις, όπως σε στρατιωτικές εφαρμογές ή σε δίκτυα VPN που χρησιμοποιούνται σε κλειστά τραπεζικά συστήματα, όπου ο διαχειριστής όλων των κλειδιών είναι ένας και μοναδικός. [30]

4.3.2 Public Key

Οι Whitfield Diffie και Martin Hellman το 1976 παρουσίασαν την κρυπτογραφική μέθοδο δημοσίου κλειδιού (public key), με σκοπό να λύσουν το πρόβλημα που δημιουργείται στην ανταλλαγή του κλειδιού της μεθόδου private key. Σε αυτή την μέθοδο, ο αποστολέας και ο παραλήπτης έχουν από ένα δημόσιο (public) και ένα ιδιωτικό (private) κλειδί. Το δημόσιο κλειδί είναι γνωστό σε όλους (μπορεί να βρεθεί σε διάφορα ευρετήρια), ενώ το ιδιωτικό κλειδί το γνωρίζει μόνο ο κάτοχός του. Σε αυτό το είδος κρυπτογράφησης δεν τίθεται θέμα ασφάλειας των καναλιών, διότι μόνον ο κατάλληλος παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα.

Η χρήση του δημοσίου κλειδιού έχει το **πλεονέκτημα της ασφάλειας**, σε αντίθεση με το ιδιωτικό κλειδί, το οποίο είναι επίφοβο να μεταδίδεται μέσω του δικτύου ή μέσω τρίτου ατόμου. Άλλο πλεονέκτημα του δημοσίου κλειδιού είναι η δυνατότητα παροχής αξιόπιστων ηλεκτρονικών υπογραφών.

Σοβαρό **μειονέκτημα** των public key αλγορίθμων αποτελεί η **μικρή ταχύτητά τους**, σε αντίθεση με τους private key αλγόριθμους, οι οποίοι είναι αισθητά γρηγορότεροι. Με βάση τα πλεονεκτήματα των δύο παραπάνω κρυπτογραφικών αλγορίθμων, έχουν δημιουργηθεί διάφορες "digital envelope" μέθοδοι, οι οποίες συνδυάζουν τις δύο ανωτέρω μεθόδους και συμπεριφέρονται πολύ ικανοποιητικά. [31]

4.3.3 Block Ciphers

Μια άλλη μέθοδος κρυπτογράφησης είναι η λεγόμενη «**Block Cipher**», η οποία επαναλαμβάνει διάφορες λειτουργίες, όπως αντικατάσταση, μετάθεση, πολλαπλασιασμό, και γραμμικούς μετασχηματισμούς δημιουργώντας έτσι ένα πολύ πιο δυνατό αλγόριθμο. Χρησιμοποιείται κυρίως σε ασύρματα δίκτυα. Η αποκρυπτογράφηση αυτής της μεθόδου γίνεται με την αντίστροφη διαδικασία με την οποία έγινε η κρυπτογράφηση. [32]

4.3.4 Data Encryption Standard - DES

Το πρότυπο Data Encryption Standard έχει αναπτυχθεί από την εταιρία IBM και αρχικά είχε την ονομασία Lucifer. Γενικά ο αλγόριθμος κρυπτογράγησης που αντιπροσωπεύει το πρότυπο αυτό, **δεν** είναι **εύκολο να δεχθεί επιθέσεις**. Από την άλλη πλευρά, έχουν βρεθεί μηχανισμοί οι οποίοι μπορούν **να τον αποκωδικοποιήσουν.** Ένας τέτοιος μηχανισμός είναι **η "brute-force attack"**, η οποία προσπαθεί να βρει όλους τους δυνατούς συνδυασμούς που μπορούν να γίνουν και άρα να βρει και τον σωστό συνδυασμό. Μια άλλη τεχνική είναι η **"sustained data analysis**", η οποία εντοπίζει τους κοινούς χαρακτήρες που υπάρχουν στα κρυπτογραφημένα μηνύματα, με αποτέλεσμα να εντοπίζουν το κλειδί με το οποίο έχουν κρυπτογραφηθεί όλα τα μηνύματα. Αν αυτοί οι χαρακτήρες έχουν μεγάλη συχνότητα εμφάνισης τότε κάποιος μπορεί να συμπεράνει με μεγάλη πιθανότατα ποια είναι αυτή η λέξη. Ο μηχανισμός αυτός είναι ένας τρόποιο αποκρυπτογράφησης του προτύπου **DES**. Η **συχνή αλλαγή των κλειδιών** είναι ο μόνος τρόπος με τον οποίο μπορεί να γίνει πιο δύσκολη η αποκρυπτογράφηση του προτύπου DES. [33]

4.3.5 Hash Functions (Συναρτήσεις Κατακερματισμού)

Οι συναρτήσεις κατακερματισμού – Hash, έχουν τη δυνατότητα να παίρνουν ένα μήνυμα, το οποίο μπορεί να έχει διαφορετικό μέγεθος κάθε φορά και να το τροποποιούν σε ένα **μήνυμα σταθερού μεγέθους**, συνήθως **128 bits** ή περισσότερα. Οι hash συναρτήσεις είναι μονόδρομες (**one way**), δηλαδή είναι πολύ δύσκολο να βρεθεί η αντίστροφη συνάρτηση ώστε να αποκωδικοποιηθούν. Συνεπώς, είναι πολύ δύσκολο να βρεθεί το κλειδί κρυπτογράφησης μιας συνάρτησης κατακερματισμού. Αυτή η **μέθοδος χρησιμοποιείται** ευρέως σε **ηλεκτρονικές υπογραφές.** [34]

4.3.6 Digital Signatures

Η χρήση των ψηφιακών υπογραφών μεγάλωσε την **αξιοπιστία** των VPNs. Με τον τρόπο αυτό πιστοποιούνται τα δεδομένα, αλλά και τα πρόσωπα μεταξύ των οποίων γίνεται η ανταλλαγή μηνυμάτων. **Οι ψηφιακές υπογραφές** είναι ένα **είδος κρυπτογράφησης** το οποίο **χρησιμοποιεί hash συναρτήσεις**. Κάθε μήνυμα χρησιμοποιεί μια συνάρτηση κατακερματισμού (hash), το μειώνει στα 128-bits και το κρυπτογραφεί με ένα κλειδί. Έτσι, δημιουργείται μια ψηφιακή υπογραφή. Στη συνέχεια, η υπογραφή αυτή μαζί με το αρχικό μήνυμα κρυπτογραφούνται ξανά και στέλνονται στον παραλήπτη. Ο παραλήπτης πρώτα αποκρυπτογραφεί το αρχικό μήνυμα, στη συνέχεια την υπογραφή του αποστολέα και τα συγκρίνει μεταξύ τους. Έτσι, μπορεί να αξιολογήσει εάν το μήνυμα που παρέλαβε είναι αυθεντικό, δηλαδή στάλθηκε από το σωστό αποστολέα. [35]

4.3.7 RSA Public – Key Αλγόριθμος

Ένας από τους πρώτους μηχανισμούς κρυπτογράφησης που χρησιμοποιεί το «δημόσιο κλειδί» (public key) είναι ο **RSA αλγόριθμος**. Αυτός ο μηχανισμός χρησιμοποιεί ένα κλειδί κρυπτογράφησης το οποίο είναι «δημόσιο» (public) και ένα «μυστικό» κλειδί αποκρυπτογράφησης το οποίο είναι κρυφό. Ο αλγόριθμος RSA δημιουργήθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman και ονομάσθηκε έτσι από τα αρχικά γράμματα των επωνύμων τους. Ο αποστολέας, που χρησιμοποιεί την RSA κωδικοποίηση, δημιουργεί και στη συνέχεια δημοσιεύει ένα δημόσιο κλειδί που βασίζεται σε δύο μεγάλους πρώτους αριθμούς, σε συνδυασμό με μια βοηθητική τιμή. Οι δύο πρώτοι αριθμοί που χρησιμοποιήθηκαν πρέπει να κρατηθούν μυστικοί. Αν το δημόσιο κλειδί που χρησιμοποιεί κάποιος για να κρυπτογραφήσει ένα κείμενο είναι αρκετά μεγάλο, μόνο κάποιος ο οποίος γνωρίζει τους πρώτους αριθμούς που χρησιμοποιήθηκαν μπορεί να αποκωδικοποιήσει το κείμενο. Ο RSA δεν χρησιμοποιείται πολύ συχνά, καθόσον είναι ένας σχετικά αργός αλγόριθμος κρυπτογράφησης. Συχνότερα, ο αλγόριθμος αυτός χρησιμοποιείται για να παρέχει ήδη κρυπτογραφημένα κλειδιά σε άλλους μηχανισμούς, ώστε να είναι πιο γρήγορη η συνολική διαδικασία. [36]

4.3.8 Pretty Good Privacy (PGP)

Είναι ένα υβριδικό κρυπτοσύστημα, καθώς συνδυάζει τον **public key αλγόριθμο** και τον **private key αλγόριθμο**. Χρησιμοποιείται σε αρκετές εφαρμογές, όπως το ηλεκτρονικό ταχυδρομείο. Το PGP λειτουργεί όπως όλα τα public key κρυπτοσυστήματα, χρησιμοποιώντας τον RSA public key αλγόριθμο και τον International Data Encryption αλγόριθμο (IDEA). Ένα IDEA κλειδί χρησιμοποιείται για κρυπτογράφηση αλλά και για αποκρυπτογράφηση του μηνύματος. Ο RSA αλγόριθμος χρησιμοποιείται για να κρυπτογραφήσει το IDEA κλειδί μαζί με το public key που χρησιμοποιεί ο παραλήπτης. Έτσι, μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Με τον τρόπο αυτό, έχουμε έναν απλό, ασφαλή και γρήγορο τρόπο για να κρυπτογραφούμε μηνύματα και να τα στέλνουμε με ασφάλεια. [37]

4.4 Επιθέσεις σε VPNs

Για κάθε είδους επίθεση που δέχεται ένα VPN πρέπει να διευκρινίσουμε πότε είναι εξωτερική επίθεση, δηλαδή παραβίαση του VPN από κάποιο εξωτερικό χρήστη, και πότε είναι εσωτερική επίθεση, δηλαδή αδυναμία του ίδιου του VPN. Τα δύο βασικά πρωτόκολλα που χρησιμοποιούνται για την υλοποίηση των VPNs, είναι *τα IPSec* και το *PPTP.*

4.5 Είδη επιθέσεων στο πρωτόκολλο Internet Protocol Security (IPSec)

Η ομάδα που δημιούργησε το IPSec πρωτόκολλο, όρισε την δομή του IP πακέτου και υλοποίησε διάφορες ασφαλείς συνδέσεις (secure associations – SA), οι οποίες από τον Νοέμβριο του 1998 έχουν καθιερωθεί ως πρότυπα και χρησιμοποιούνται στις VPN επικοινωνίες. Το IPSec ορίζει ένα σύνολο πρωτοκόλλων και κρυπτογραφικών αλγορίθμων για δημιουργία ασφαλών συνδέσεων με χρήση μιας IP διεύθυνσης. Όπως τα άλλα πρωτόκολλα ασφαλείας, έτσι και το IPSec μπορεί να δεχθεί επιθέσεις.

Μερικά είδη επιθέσεων που μπορεί να δεχθεί το πρωτόκολλο IPSec είναι τα εξής:

- ***Επιθέσεις κατά της διαχείρισης κλειδιού***

Ένα πρόβλημα παρουσιάζεται στον τρόπο που το πρωτόκολλο διαχείρισης κλειδιού (IKE) διαχειρίζεται τα κρυπτογραφικά κλειδιά στο πρωτόκολλο του IPSec. Στις προδιαγραφές του πρωτοκόλλου διευκρινίζεται πως αυτά τα κλειδιά πρέπει να ανταλλάσσονται μεταξύ των δύο άκρων που επικοινωνούν, αλλά συνήθως αναφέρεται μόνο για την αρχή της επικοινωνίας και όχι για το τέλος της. Λόγω του ότι υπάρχει μηχανισμός λήξης στις συναλλαγές πληροφοριών με χρήση του public key, έχει διαπιστωθεί ότι **δεν υπάρχει interoperability** μεταξύ των διάφορων προμηθευτών (ventors)**.**

Επίσης, σύμφωνα με τις προδιαγραφές του IKE, αν κατά την διάρκεια της επικοινωνίας κάποιο από τα άκρα της διακόψει την επικοινωνία, τότε δεν υπάρχει τρόπος να αντιληφθεί το άλλο άκρο ότι έχει γίνει διακοπή της επικοινωνίας και μπορεί να συνεχίζει να στέλνει πακέτα. Δηλαδή, αν το ένα άκρο εξακολουθεί να στέλνει πακέτα, τότε μπορεί να παρεμβληθεί κάποιος άλλος χρήστης και να αποκρυπτογραφήσει τα δεδομένα, αν στα αποστελλόμενα πακέτα χρησιμοποιούνται κλειδιά τα οποία είναι εύκολο να προβλέψει και να «σπάσει» κάποιος.

Ένα από τα αυτά τα κλειδιά είναι η περίπτωση όπου τα **κλειδιά είναι στατικά** κατά την διάρκεια της επικοινωνίας και δεν υπάρχει μηχανισμός για ανταλλαγή αυτών των κλειδιών. Ένα άλλο σημαντικό μειονέκτημα για το IPSec είναι η **δυσκολία χειρισμού του μεγάλου αριθμού των κρυπτογραφικών κλειδιών στα μεγάλα δίκτυα**. Μία λύση σε αυτό το πρόβλημα είναι το ***Certificate Enrollment Protocol (CEP)*** το οποίο έχει αναπτυχθεί από την Cisco και την VeriSign και **επιτρέπει την ανταλλαγή μεγάλου αριθμού κλειδιών.**

Τέλος, το IPSec **δεν έχει μηχανισμό για πιστοποίηση χρηστών** όπως δικαιώματα πρόσβασης, πιστοποίηση, κ.ο.κ. Λόγω του ότι αρχικά είχε σχεδιαστεί για LAN-to-LAN VPN, **δεν παρέχει μηχανισμό υποστήριξης πελατών**. Με σκοπό το IPSec να μπορεί να παρέχει αυτό τον μηχανισμό, έχουν γίνει τροποποιήσεις στο αρχικό πρότυπο.

4.6 Είδη επιθέσεων στο πρωτόκολλο Point-to-Point Tunneling Protocol (PPTP)

Το PPTP είναι ένας συνδυασμός του Point-to-Point Protocol και του Transmission Control Protocol / Internet Protocol (TCP/IP). Το PPTP συνδυάζει τα χαρακτηριστικά του PPP (όπως η συμπίεση πακέτων δεδομένων) και του TCP/IP (κυρίως τη δυνατότητα για δρομολόγηση των πακέτων στο Internet). **Μαζί με το IPSec είναι ένα από τα κύρια VPN πρωτόκολλα που χρησιμοποιούνται σήμερα**.

Χρησιμοποιεί το **Generic Routing Protocol (GRE)** για **μεταφορά** των P**PP πακέτων.** Το πρωτόκολλο PPTP χαρακτηρίζεται από δύο είδη πακέτων που χρησιμοποιεί στην ανταλλαγή δεδομένων: τα "**data packets"** και "**control packets"**. Τα control packets χρησιμοποιούνται για έλεγχο των δεδομένων που ανταλάσσονται, ενώ τα data packets για να μεταφέρουν τα δεδομένα του χρήστη. Τα data packets είναι πακέτα τα οποία έχουν υποστεί την διαδικασία της ενθυλάκωσης (encapsulation), δηλαδή διαδικασία με την οποία τα καθ'αυτά δεδομένα προστίθεται σε άλλα

δεδομένα, όπως κάποια επικεφαλίδα, χρησιμοποιώντας το πρωτόκολλο Internet Generic Routing Encapsulation Version 2 (GRE v2). [24]

Το PPTP, όπως και το IPSec, έχει μειονεκτήματα, όπως το ότι δεν υποστηρίζει αλγόριθμους για encryption και authentication. Αυτό γίνεται από άλλα πρωτόκολλα.

Μια επίθεση που μπορεί να δεχθεί το πρωτόκολλο PPTP, είναι στην επιμέρους διαδικασία που εφαρμόζει με το Generic Routing Encapsulation (GRE). Τα πακέτα του GRE μπορούν να μεταφέρουν μαζί τους ένα αριθμό που υποδεικνύει τη σειρά στην οποία βρίσκονται στην ακολουθία πακέτων που αποστέλλεται, ένα “acknowledge” για κάθε αριθμό, ενώ για την αποφυγή της συμφόρησης μπορεί να χρησιμοποιηθεί και η παράμετρος του χρόνου αποστολής. Όμως, **αν κάποιος αποσυγχρονίσει την ακολουθία των πακέτων, τότε μπορεί να εξαπατήσει το GRE**. Επίσης, το GRE δεν έχει τρόπο να αντιδράσει σε κακή ή διπλή ακολουθία αριθμών. Αυτό πιθανότατα να αγνοηθεί αλλά τότε τα πακέτα PPP μπορούν να αλλοιωθούν.

Επίσης, ένα μειονέκτημα του Point-to-Point Tunneling Protocol (PPTP) είναι ότι βασίζεται στο πρωτόκολλο Point-to-Point (PPP) και πριν από κάθε επικοινωνία το κάνει εγκατάσταση και αρχικοποιεί τις παραμέτρους επικοινωνίας. Όμως, αφού το Point-to-Point Protocol (PPP) **δεν έχει μηχανισμό πιστοποίησης** κατά τη διάρκεια της μετάδοσης αυτών των PPP πακέτων μπορεί κάποιος ενδιάμεσος να εξαπατήσει το σύστημα και να πάρει τις πληροφορίες που ανταλλάσονται.

ΚΕΦΑΛΑΙΟ 5: ΠΡΟΣΟΜΟΙΩΣΕΙΣ

5.1 Ανάλυση του εργαλείου Cisco Packet Tracer

Το Cisco Packet Tracer είναι ένα **πρόγραμμα προσομοίωσης δικτύων** που έχει δημιουργηθεί από την εταιρία Cisco. Το εργαλείο αυτό επιτρέπει στους χρήστες να σχεδιάζουν οποιαδήποτε τοπικά δίκτυα ή δίκτυα WAN και Cloud από το μηδέν. Η δημιουργία δικτυακών τοπολογιών, η επιλογή από μία πληθώρα συσκευών όπως υπολογιστές, laptops, tablets, δρομολογητές, μεταγωγείς, εξυπηρετητές και συνδέσεις με διαφορετικά είδη καλωδίων, **δημιουργούν την αίσθηση ενός πραγματικού περιβάλλοντος δικτύωσης.** Το γραφικό περιβάλλον του το καθιστά εύκολο στη χρήση ενώ η προσομοίωση γίνεται σε πραγματικές συσκευές με πραγματικές συνθήκες

Το Cisco Packet Tracer είναι διαθέσιμο για λειτουργικά Windows και Linux, αλλά και για κινητά τηλέφωνα. Για να κατεβάσει κανείς τον προσομοιωτή της Cisco χρειάζεται να κάνεις εγγραφή στο Cisco Networking Academy. Το CPT διαθέτει μια σειρά από προσομοιωμένα πρωτόκολλα στρώματος εφαρμογής, όπως HTTP και DNS, καθώς και βασικά πρωτόκολλα δρομολόγησης με RIP, OSPF και EIGRP.

Το γραφικό περιβάλλον του CPT είναι πολύ πρακτικό και πολύ εύκολο στη χρήση. Παρέχει ρεαλισμό στην προσομοίωση, καθώς προσομοιώνει πραγματικές συσκευές σε πραγματικές συνθήκες. Εκτός από το γραφικό περιβάλλον, υπάρχει επίσης και την Command List (CLI), η οποία επιτρέπει τον προγραμματισμό των δικτυακών συσκευών.

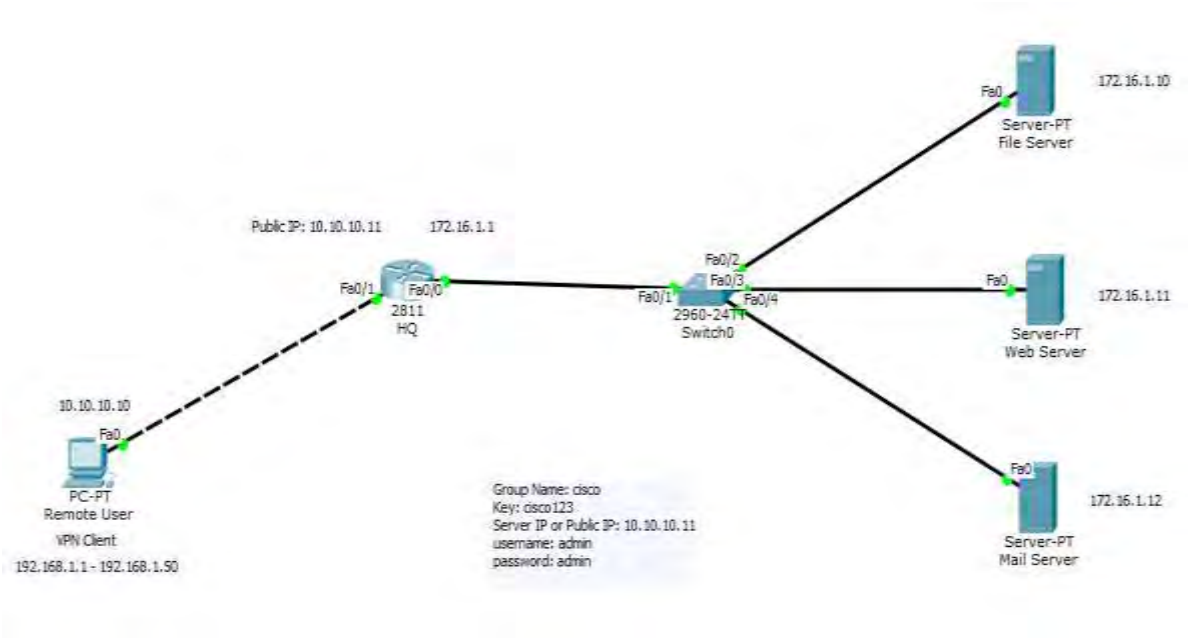
Το Cisco Packet Tracer 6.3 έχει κυκλοφορήσει στις 22 Δεκεμβρίου το 2015 από τη Cisco. Πρόκειται για μια έκδοση συντήρησης με netacad login ενεργοποιημένη κατά την εκκίνηση της εφαρμογής. Αντικατέστησε το Cisco Packet Tracer 6.2 Φοιτητών και Cisco Packet Tracer 6.2 Instructor. Το Cisco Packet Tracer 6.2 περιλαμβάνει ASA 5505 τείχους προστασίας με τη διαμόρφωση της γραμμής εντολών (αλλά όχι Adaptive Συσκευή Ασφαλείας Manageror KKK εργαλεία). Περιλαμβάνει επίσης ένα NetFlow συλλέκτη ως Desktop εφαρμογή στη συσκευή διακομιστή, πρωτόκολλα δρομολόγησης για το IPv6 (OSPFv3, EIGRPv6, RIPng), DHCP snooping εντολές, το IPv6 CEF, IPSEC.

Το Packet Tracer 6.2 εισήγαγε την υποστήριξη τηλεφωνίας 3G / 4G, καθώς και ένα νέο Cisco 819 ISR router με ενσωματωμένο ασύρματο σημείο πρόσβασης. Σε αυτήν την έκδοση προστέθηκαν επίσης και οι βελτιώσεις OSPF και EIGRP. Το Packet Tracer 7.0 έχει κυκλοφορήσει στις 17 Ιουνίου 2016. Αυτή είναι μια νέα σημαντική έκδοση που περιλαμβάνει 3 νέους δρομολογητές Cisco (819IOX, 829, 1240 routers), ένα νέο IE2000 διακόπτη industral και τεράστια βελτιωμένα πρωτόκολλα. Ακόμη έχουν προστεθεί οι δυνατότητες Python και javascript scripting. [38]

5.2 Προσομοίωση 1: Σύνδεση απομακρυσμένου χρήστη μέσω VPN σε ένα απλοποιημένο δίκτυο.

Σκοπός της προσομοίωσης αυτής είναι **η αναλυτική παρουσίαση και περιγραφή της διαδικασίας σύνδεσης ενός απομακρυσμένου χρήστη (Remote User) σε ένα απλό VPN.** Με τον τρόπο αυτό θα εστιάσουμε περισσότερο στην **ασφάλεια** που δημιουργεί ένα VPN, καθώς χωρίς αυτό ο χρήστης δεν θα μπορεί να έχει πρόσβαση στο υπόλοιπο δίκτυο.

Η προσομοίωση έγινε με τη χρήση του λογισμικού **Cisco Packet Tracer** (version 6.3). Στην παρακάτω εικόνα, παρουσιάζεται ένα απλοποιημένο δίκτυο που στήθηκε προκειμένου να αναλυθεί ο τρόπος σύνδεσης ενός απομακρυσμένου χρήστη μέσω VPN σε ένα άλλο δίκτυο. Φυσικά το δίκτυο μπορεί να επεκταθεί και να εξυπηρετήσει περισσότερους χρήστες.



Εικόνα 20: Σύνδεση απομακρυσμένου χρήστη μέσω VPN σε ένα απλοποιημένο δίκτυο.

Στην προσομοίωση χρησιμοποιήσαμε ένα Cisco Router 2811 και ένα Switch 2960. Προκειμένου να λειτουργήσει σωστά ένα δίκτυο, πρέπει εκτός από τον κατάλληλο εξοπλισμό – ο οποίος θα προγραμματιστεί σωστά, να κάνουμε και τις απαραίτητες συνδέσεις μεταξύ τους. Το Cisco Packet Tracer διαθέτει στο χρήστη όλους τους δυνατούς τρόπους σύνδεσης. Χρησιμοποιήθηκε κατά κύριο λόγο copper straight-through καλώδιο, δηλαδή καλώδιο χαλκού απευθείας εξόδου. Ο Cisco Router (HQ) έχει ρυθμιστεί ώστε να μοιράζει διευθύνσεις στο δίκτυο. Να τονίσουμε ότι στη συγκεκριμένη προσομοίωση θα συνδέσουμε τον απομακρυσμένο χρήστη μέσω καλωδίου με το υπόλοιπο δίκτυο (copper cross-over). Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά όλες οι συνδέσεις που έγιναν μεταξύ των συσκευών του δικτύου.

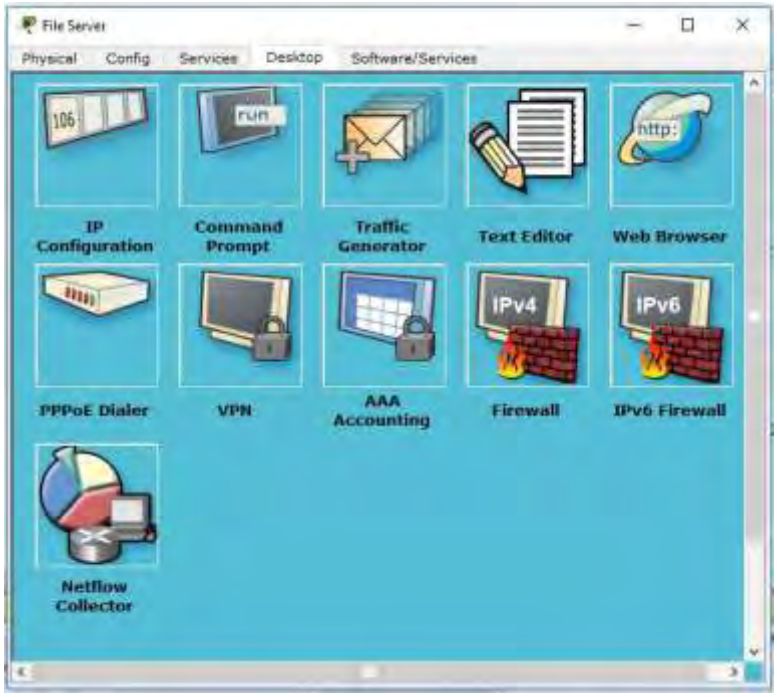
Αφετηρία		**Τερματισμός**		**Τύπος Καλωδίου**
Συσκευή	**Προφίλ**	**Συσκευή**	**Προφίλ**	
Cisco Router (HQ)	FastEthernet 0/0	Switch	FastEthernet 0/1	Copper straight-through
Switch	FastEthernet 0/2	File Server	FastEthernet 0	Copper straight-through
Switch	FastEthernet 0/3	Web Server	FastEthernet 0	Copper straight-through
Switch	FastEthernet 0/4	Mail Server:	FastEthernet 0	Copper straight-through
Cisco Router (HQ)	FastEthernet 0/1	Remote User	FatsEthernet0	Copper Cross-Over

Πίνακας 3: Συνδεσμολογία Δικτύου 1

Στον παραπάνω πίνακα, φαίνονται και οι συσκευές που έχουν προστεθεί στο δίκτυο, δηλαδή οι Servers. Οι συσκευές αυτές που τοποθετούνται στα άκρα του δικτύου ονομάζονται End Devices. Άρα προσθέτουμε τρεις (3) συσκευές Generic για Servers και τους συνδέουμε με το switch με copper straight-through καλώδιο, όπως φαίνεται και παραπάνω. Τέλος, φαίνεται ότι υπάρχει ένας Remote User που ουσιαστικά στο σχέδιο του δικτύου της εικόνας 21, βλέπουμε ότι απεικονίζεται με έναν υπολογιστή.

Στην συνέχεια ορίζουμε διεύθυνση ip σε κάθε Server, όπως φαίνεται στην παρακάτω εικόνα:

Click σε κάθε Server -> Desktop -> IP Configuration



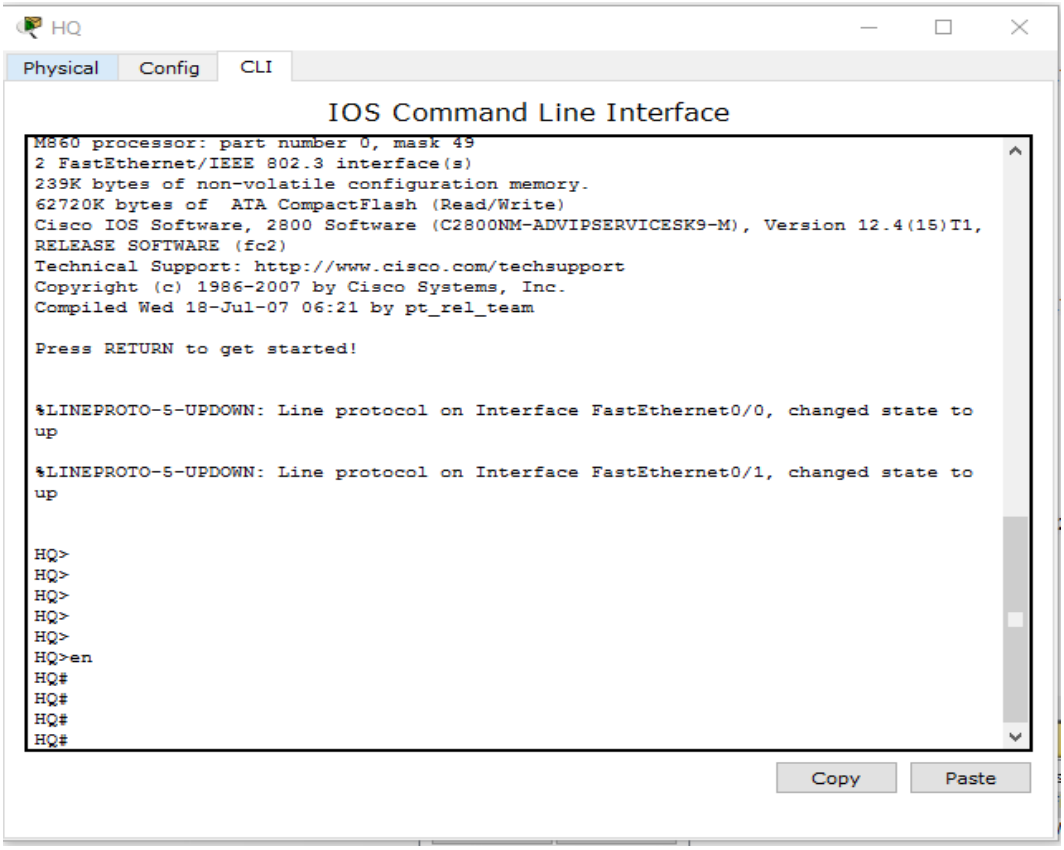
Εικόνα 21: IP Configuration

Το ρόλο του Gateway, διαδραματίζει ο Cisco Router 2811. Στον παρακάτω πίνακα παρουσιάζονται οι διεύθυνση ip που έχει δοθεί σε κάθε συσκευή.

Συσκευή	IP
Cisco Router (HQ)	Int0/0: 172.16.1.1
	Int0/1: 10.10.10.11
File Server	172.16.1.10
Web Server	172.16.1.11
Mail Server	172.16.1.12
Remote User	10.10.10.10

Πίνακας 4: Διευθύνσεις Ips Δικτύου 1

Παρακάτω θα παρουσιάσουμε την παραμετροποίηση του δικτύου και πιο συγκεκριμένα του router, που είναι υπεύθυνο και για την δρομολόγηση των διευθύνσεων στο δίκτυο. Θα παραμετροποιήσουμε το VPN με χρήση του πρωτοκόλλου IPsec. Για να παραμετροποιήσουμε το cisco router θα χρησιμοποιήσουμε το "Command Line Interface", δηλαδή θα το προγραμματίσουμε μέσω εντολών, οι οποίες αναλύονται παρακάτω. Το περιβάλλον προγραμματισμού φαίνεται στην παρακάτω εικόνα:



Εικόνα 22: Command Line Interface

Στον παρακάτω πίνακα φαίνονται οι εντολές που δόθηκα στον Cisco Router προκειμένου να το προγραμματίσουμε:

Εντολή	Περιγραφή
Router>**enable**	Εισαγωγή σε privilege mode, όπου μπορούμε να δούμε όλα τα configurations που έχουνε γίνει στο router αλλά και να το προγραμματίσουμε.
Router#**configure terminal**	Εισαγωγή σε Global Configuration Mode, όπου γίνεται ο προγραμματισμός του router
Router (config)#**hostname HQ**	Δίνουμε όνομα στο router (Στην περίπτωσή μας το ονομάζουμε HQ).

HQ(config)#**int f0/0**	Ρύθμιση του fast ethernet interface. Το συγκεκριμένο προφίλ είναι προς την πλευρά του switch.
HQ(config-if)#**ip address 172.16.1.1 255.255.255.0**	Ορισμός διεύθυνσης IP και μάσκα υποδικτύωσης (subnet mask) που θα έχει το serial interface. Η IP και το subnet mask που θα βάλουμε εξαρτάται και από την IP που μας έχουν δώσει και το subnetting που έχει γίνει. Ορισμός IP και subnet mask διεύθυνσης προς την πλευρά του switch.
HQ(config-if)#**no shutdown**	Η εντολή no shutdown χρησιμοποιείται για να ενεργοποιήσει το interface.
HQ(config-if)#**int f0/1**	Ρύθμιση του fast ethernet interface προς την πλευρά του Remote User.
HQ(config-if)#ip address 10.10.10.11 255.255.255.0	Ορισμός IP και subnet mask διεύθυνσης προς την πλευρά του Remote User.
HQ(config-if)#no shutdown	Ενεργοποίηση του interface f0/1.
	Configure VPN Remote Access
Βήμα 1	***Ορισμός aaa***
HQ(config)#**aaa new-model**	Τα τρία aaa, χρησιμοποιείται για την ασφάλεια του δικτύου, δηλαδή απαγορεύει στους μη διαπιστευμένους χρήστες να εισέρχονται και να χρησιμοποιούν το δίκτυο.
HQ(config)#**aaa authentication login abc1 local**	Το πρώτο “a” σχετίζεται με το “authentication”. Η πιστοποίηση της ταυτότητας των χρηστών των παρεχόμενων υπηρεσιών / εφαρμογών (authentication). (abc1 local είναι το όνομα της λίστας “authentication”).
HQ(config)#**aaa authorization network abc2 local**	Το δεύτερο “a” σχετίζεται με το “authorization”. Η εφαρμογή αποτελεσματικών πολιτικών ασφάλειας για τον έλεγχο της πρόσβασης των χρηστών στις εφαρμογές και τα δεδομένα (authorization) με βάση συγκεκριμένα δικαιώματα και σε πολλαπλά επίπεδα. (abc2 local είναι το όνομα της λίστας “authorization”).
HQ(config)#**username admin password admin**	Ορισμός username και password με τα οποία μπορεί να πιστοποιηθεί κάποιος χρήστης και να εισέλθει στο δίκτυο.

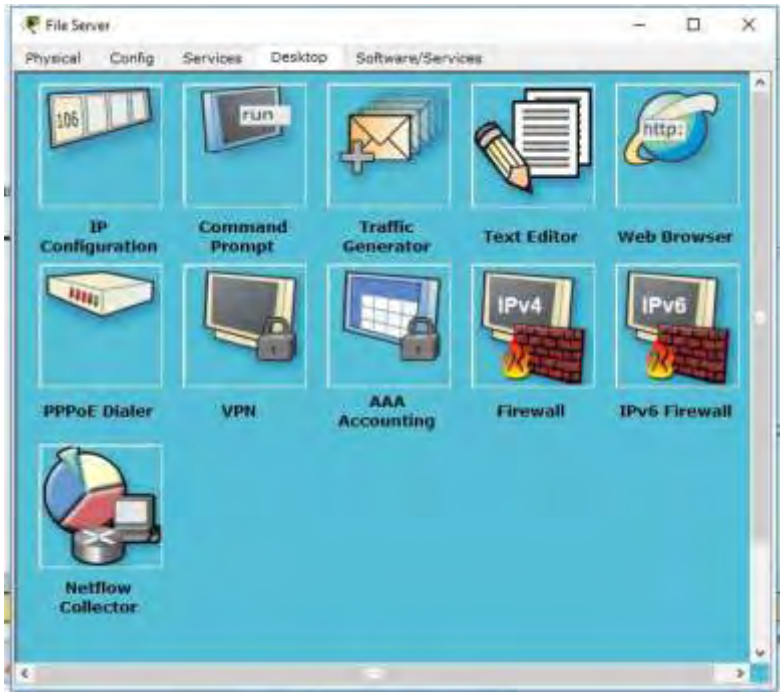
Βήμα 2	***Δημιουργία ISAKMP***
HQ(config)#**Crypto isakmp policy 10**	Ορίζει το βαθμό “priority” της πολικής προστασίας που θα εφαρμοστεί <1-10000>, καθώς και της κωδικοποίησης με τα κλειδιά με τα οποία θα ανταλλάσσονται τα δεδομένα μέσα στο VPN.
HQ(config-isakmp)#**encryption 3des**	Υπάρχουν τρία ήδη κωδικοποίησης (encryption): 3DES - Three key triple DES, AES - Advanced Encryption Standar, DES - Data Encryption Standard (56 bit keys).
HQ(config-isakmp)#**hash md5**	Υπάρχουν δύο είδη αλγορίθμων ασφαλείας: md5 - Message Digest 5, sha - Secure Hash Standard
HQ(config-isakmp)#**authentication pre-share**	Ο όρος “Pre-shared” σημαίνει ότι τα μέρη που ανταλλάσσουν μεταξύ τους δεδομένα, πρέπει να συμφωνήσουν σε ένα κοινό – μυστικό κλειδί που γίνεται μέρος της πολιτικής IPSec.
HQ(config-isakmp)#**group 2**	Ο Diffie-Hellman είναι αλγόριθμος ανταλλαγής Δημοσίου Κλειδιού (Public Key Algorithm) και αποτελείται από τρία group (1,2,5)
Βήμα 3	***Δημιουργία IP Pool***
HQ(config)#**ip local pool VPNPOOL 192.168.1.1 192.168.1.50**	Ορίζει το εύρος των διευθύνσεων οι οποίες είναι διαθέσιμες να ανατεθούν σε κάθε χρήστη που συνδέεται στο VPN, καθώς και το όνομα του “pool”.
Βήμα 4	***Δημιουργία isakmp key***
HQ(config)#**crypto isakmp client configuration group cisco**	Ορίζει το όνομα του group ασφαλείας (cisco) που πρέπει να εισάγει ο χρήστης που θα συνδεθεί στο VPN.
HQ(config-isakmp-group)#**key cisco123**	Στο παραπάνω group, ορίζουμε τον κωδικό (cisco123).
HQ(config-isakmp-group)#**pool VPNPOOL**	Ορίζουμε το όνομα του pool που θέσαμε νωρίτερα (VPNPOOL).
Βήμα 5	***Δημιουργία crypto ipsec transform-set***
HQ(config)#**crypto ipsec transform-set set1 esp-3des esp-md5-hmac**	Ως “set1” ορίζουμε το όνομα του “transform set” που δημιουργούμε. Ουσιαστικά το “transform set” είναι ο συνδυασμός των πρωτοκόλλων ασφαλείας που θα χρησιμοποιήσουμε. Θέτουμε ότι έχουμε ορίσει και πιο πάνω. Έτσι ορίζουμε την ασφάλεια IPSec.
HQ(config)#**crypto dynamic-map map1 10**	Δημιουργία ενός δυναμικού χάρτη (dynamic-map) με το όνομα map1 και σειρά εισαγωγής στο δυναμικό χάρτη 10.
HQ(config-crypto-map)#**set transform-set set1**	Ορίζουμε το set1 ως transform-set.
Βήμα 6	***Δημιουργία crypto Map***
HQ(config)#**crypto map map1**	Ορίζουμε στον Remote User – Client να συνδέεται – απαντάει στο

client configuration address respond	δίκτυο όταν συνδέεται στο VPN χρησιμοποιώντας τις ρυθμίσεις που κάναμε μέχρι τώρα (IPSec).
HQ(config)#**crypto map map1 client authentication list abc1**	Ορίζουμε ως authentication list την abc1 και το συσχετίζουμε με το crypto map στον Remote User.
HQ(config)#**crypto map map1 isakmp authorization list abc2**	Ορίζουμε ως authorization list την abc1 και το συσχετίζουμε με το crypto map.
HQ(config)#**crypto map map1 10 ipsec-isakmp dynamic map1**	Ορίζουμε στο crypto map τις ρυθμίσεις που κάναμε παραπάνω.
Βήμα 7	***Εφαρμογή crypto Map***
HQ(config)#**int f0/1**	Εισαγωγή στο interface του Remote User
HQ(config-if)#**crypto map map1**	Εφαρμογή του crypto Map που δημιουργήσαμε (*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON).

Πίνακας 5: Εντολές προγραμματισμού στο Cisco Router

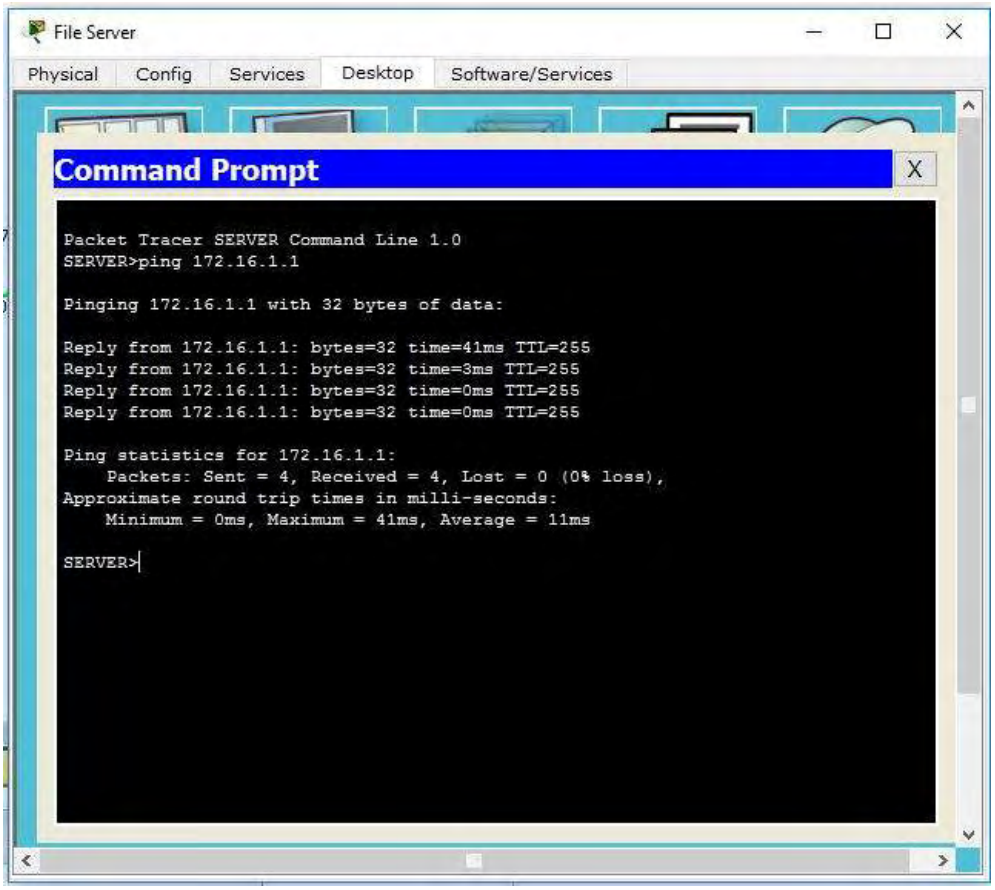
Δοκιμές:

Χρησιμοποιώντας τη γραμμή εντολών (command prompt) στο File Server, όπως φαίνεται στην παρακάτω εικόνα, δοκιμάζω εάν έχω πρόσβαση κάνοντας χρήση της εντολής “ping” στο Cisco Router.



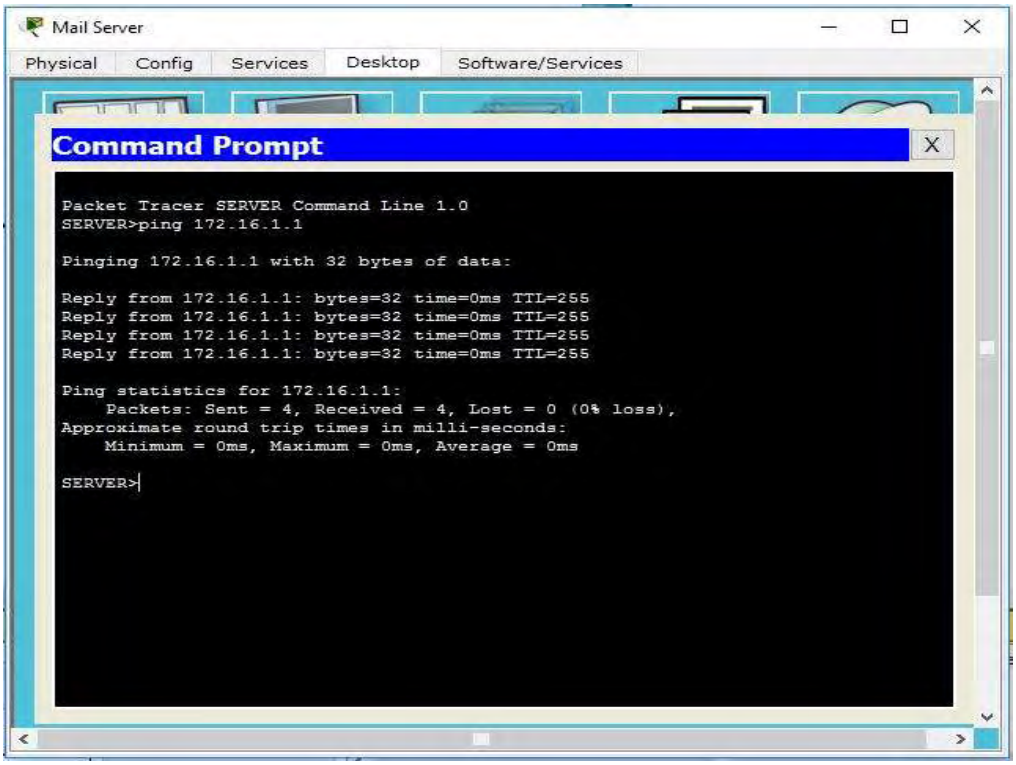
Εικόνα 23: Menu File Server Δίκτυο 1

Στον προσομοιωτή ο χρήστης θα πρέπει να: Επιλέξει το File Server -> Desktop -> Command Prompt. Παρατηρούμε ότι υπάρχει επικοινωνία μεταξύ των δύο άκρων (βλ. την παρακάτω εικόνα).

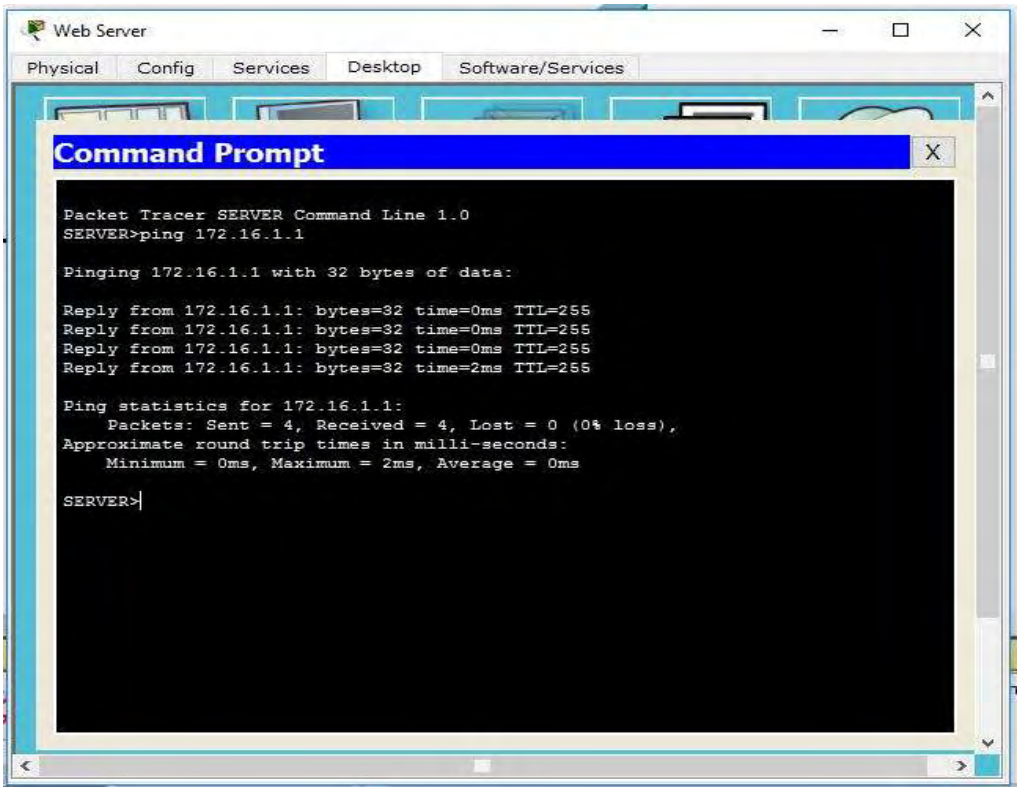


Εικόνα 24: Ping από το File Server στο Cisco Router.

Ακολουθώ την ίδια διαδικασία για να ελέγξω την επικοινωνία από κάθε server με το Cisco Router. Στις παρακάτω εικόνες φαίνεται ότι υπάρχει επικοινωνία.



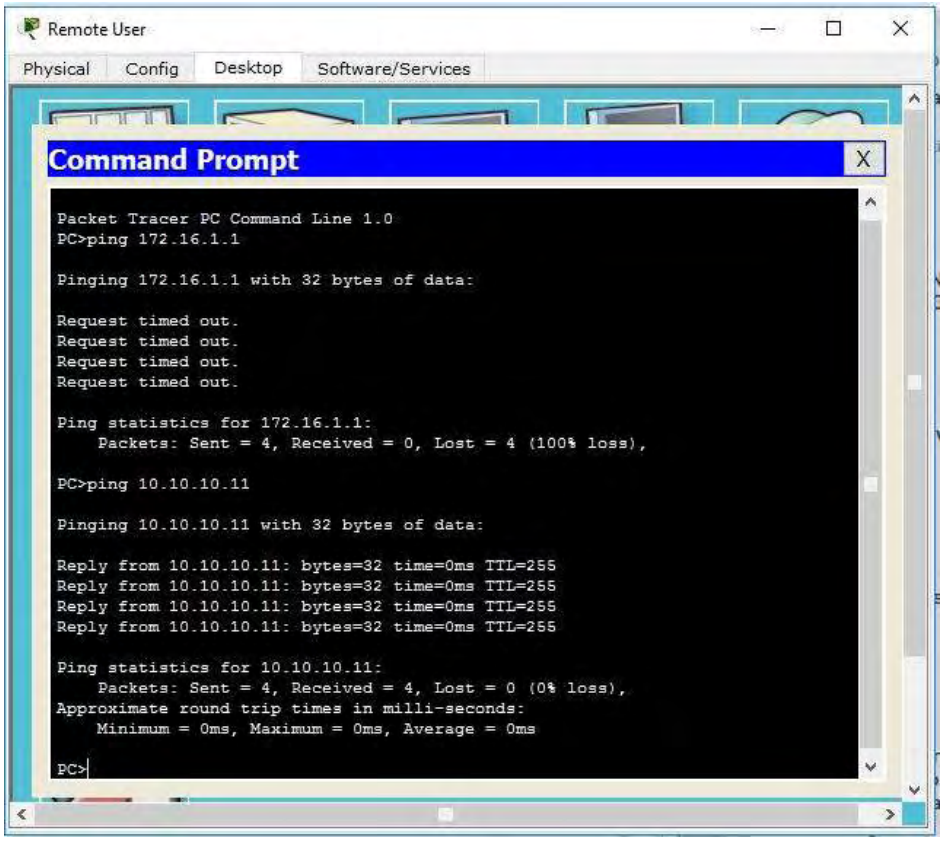
Εικόνα 25: Ping από το Mail Server στο Cisco Router.



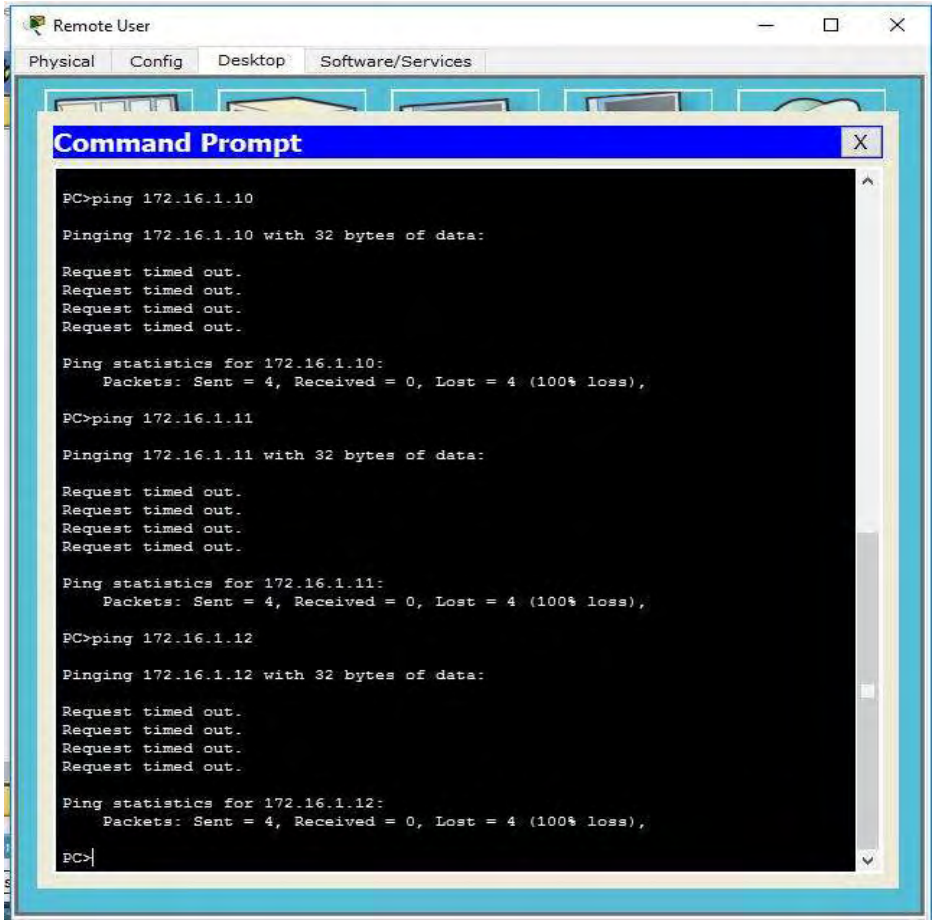
Εικόνα 26: Ping από το Web Server στο Cisco Router.

Τέλος, κάνω ping από το PC - Remote User στο cisco router. Παρατηρούμε, (Εικόνα 26) ότι απαντάει μόνο στο interface f0/1. Με το interface f0/0 δεν υπάρχει επικοινωνία. Όμοια δοκιμάζω να κάνω ping από το PC - Remote User στους Servers (Εικόνα 44). Βλέπουμε ότι και στην περίπτωση αυτή δεν υπάρχει επικοινωνία.

Άρα, το δίκτυό μας λειτουργεί σωστά, καθώς ο απομακρυσμένος χρήσης δεν έχει απευθείας πρόσβαση στο εσωτερικό δίκτυο που έχουμε στήσει. Η επικοινωνίας θα αποκατασταθεί μόνο όταν ο απομακρυσμένος χρήστης συνδεθεί στο cisco router μέσω του VPN, οπότε θα συνδεθεί μέσω του τούνελ που θα σχηματιστεί στην άλλη πλευρά του δικτύου προς τους server. Πρέπει να σημειωθεί ότι με τον τρόπο αυτό έχουμε δημιουργήσει ένα ασφαλές δίκτυο.



Εικόνα 27: Ping από το Remote User στο Cisco Router.

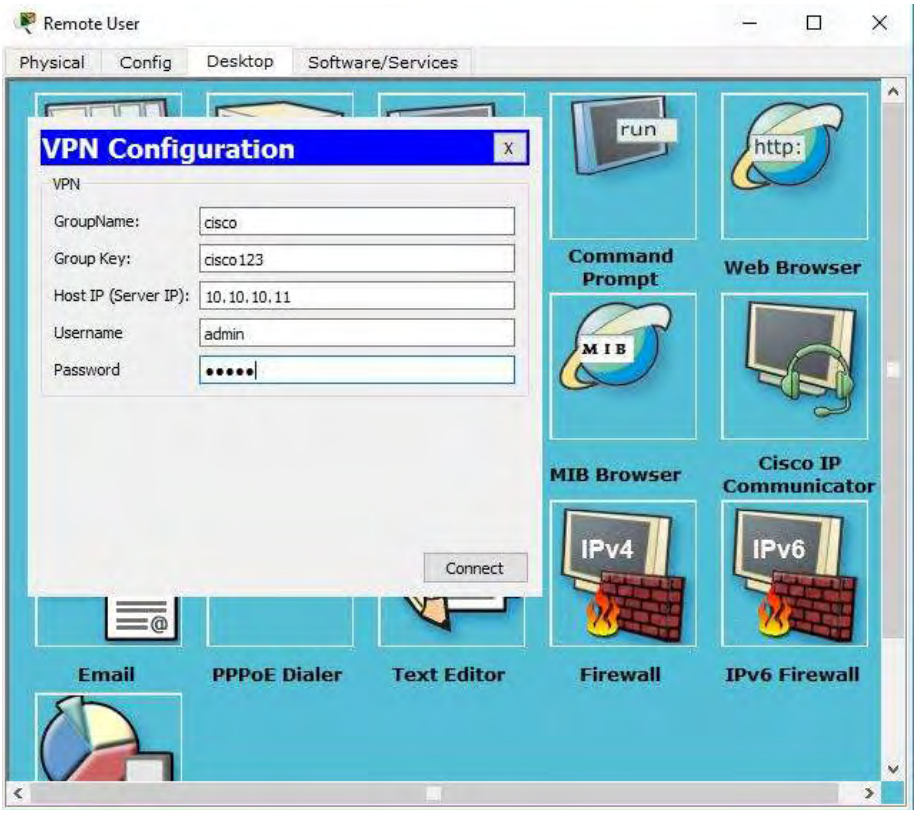


Εικόνα 28: Ping από το Remote User στους Servers.

Άρα, για να μπορέσει ο απομακρυσμένος χρήστης να έχει πρόσβαση στο δίκτυο θα πρέπει να συνδεθεί στο VPN. Στις παρακάτω εικόνες παρουσιάζεται ο τρόπος σύνδεσης του υπολογιστή του Remote User στο VPN.

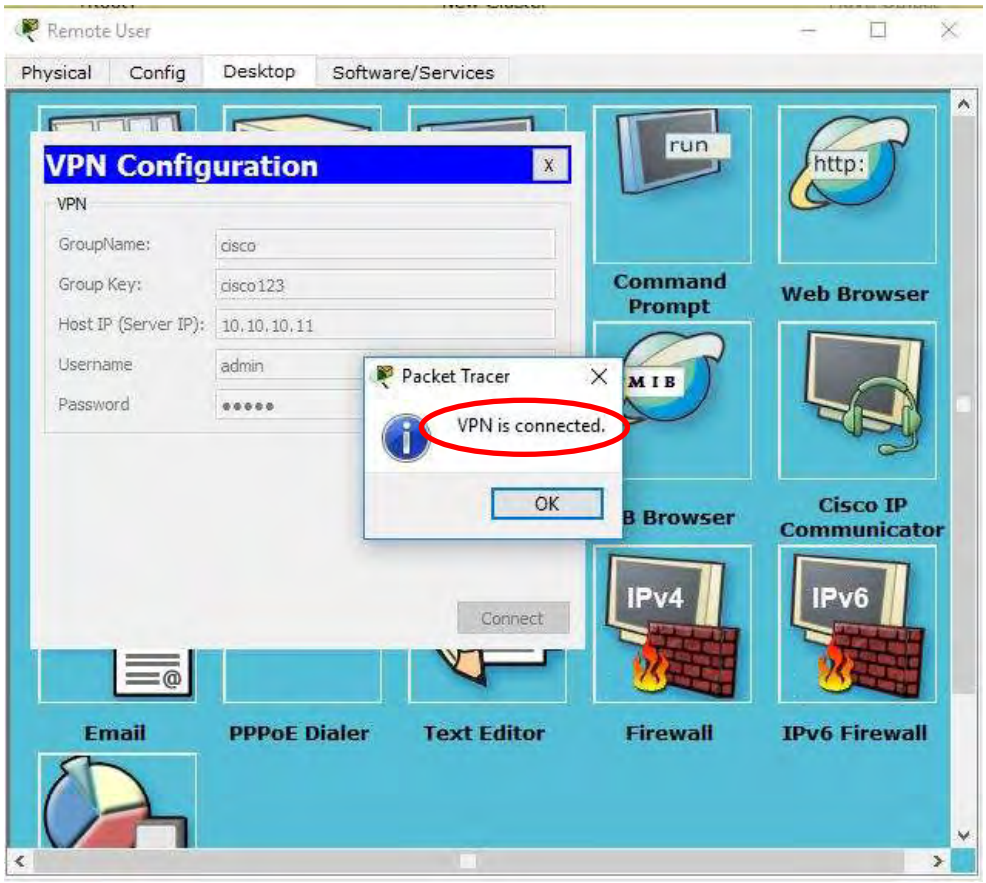
Εικόνα 29: Remote User Δίκτυο 1.

Στο πρόγραμμα προσομοίωσης η σύνδεση γίνεται ως εξής: Remote User -> Desktop -> VPN.



Εικόνα 30: VPN Configuration Δίκτυο 1.

Θα πρέπει ο χρήστης να εισάγει τα σωστά credentials όπως αυτά τα έχουμε ορίσει στον προγραμματισμό του cisco router, προκειμένου να συνδεθεί με επιτυχία στο VPN.



Εικόνα 31: VPN Συνδεδεμένο Δίκτυο 1.

Τώρα δοκιμάζω εκ νέου ping από το Remote User στους απομακρυσμένους Servers. Παρατηρούμε, ότι πλέον υπάρχει επικοινωνία μεταξύ των δυο άκρων. Η IP του Client – Remote User φαίνεται στην εικόνα 30. Στον απομακρυσμένο χρήστη έχει δοθεί μια διεύθυνση από το VPN POOL που έχουμε ορίσει.

Στην εικόνα 31 φαίνεται ότι πλέον μετά την δημιουργία του VPN υπάρχει επικοινωνία με τους servers. Αποσυνδέω το VPN και εξετάζω ξανά την επικοινωνία. Παρατηρούμε ότι χάθηκε πάλι η επικοινωνία.

Τέλος, όταν ο Remote User είναι συνδεδεμένος στο VPN, μπορώ να το δω αυτό και στο cisco router HQ χρησιμοποιώντας την παρακάτω εντολή:

HQ#**show crypto isakmp sa**

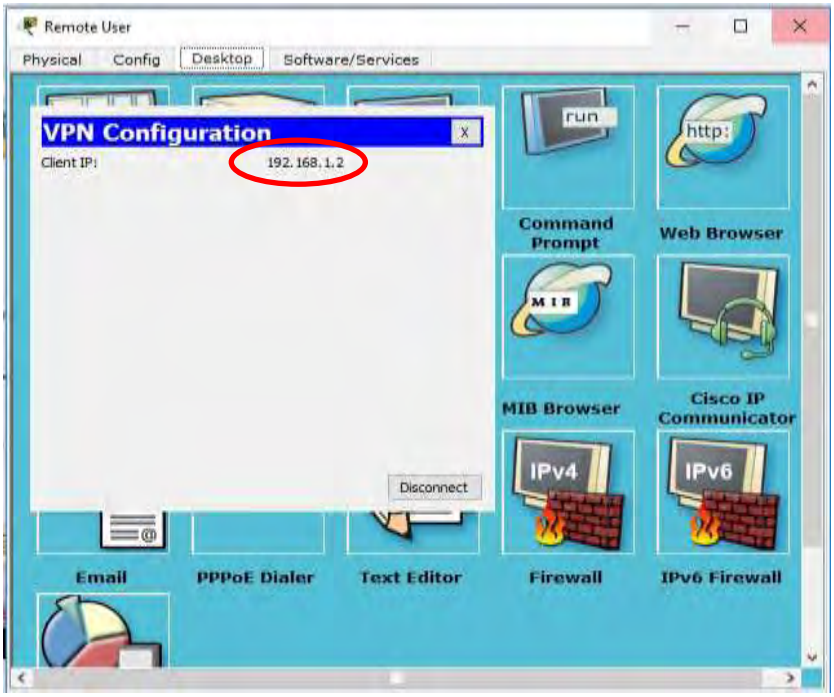
IPv4 Crypto ISAKMP SA

dst src state conn-id slot status

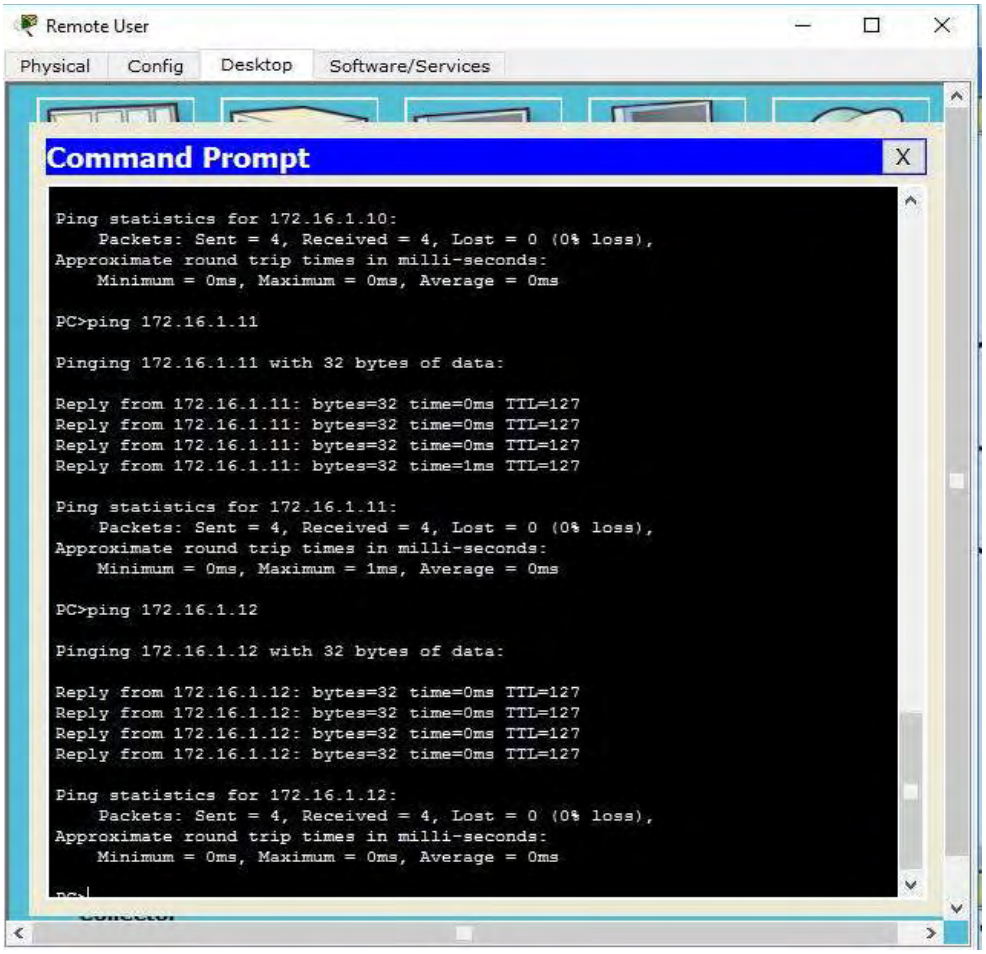
10.10.10.10 10.10.10.11 QM_IDLE 1052 0 ACTIVE

IPv6 Crypto ISAKMP SA

Παρατηρούμε δηλαδή παραπάνω ότι έχουμε δημιουργήσει εάν VPN αναμεσά στον client και στο cisco router HQ.

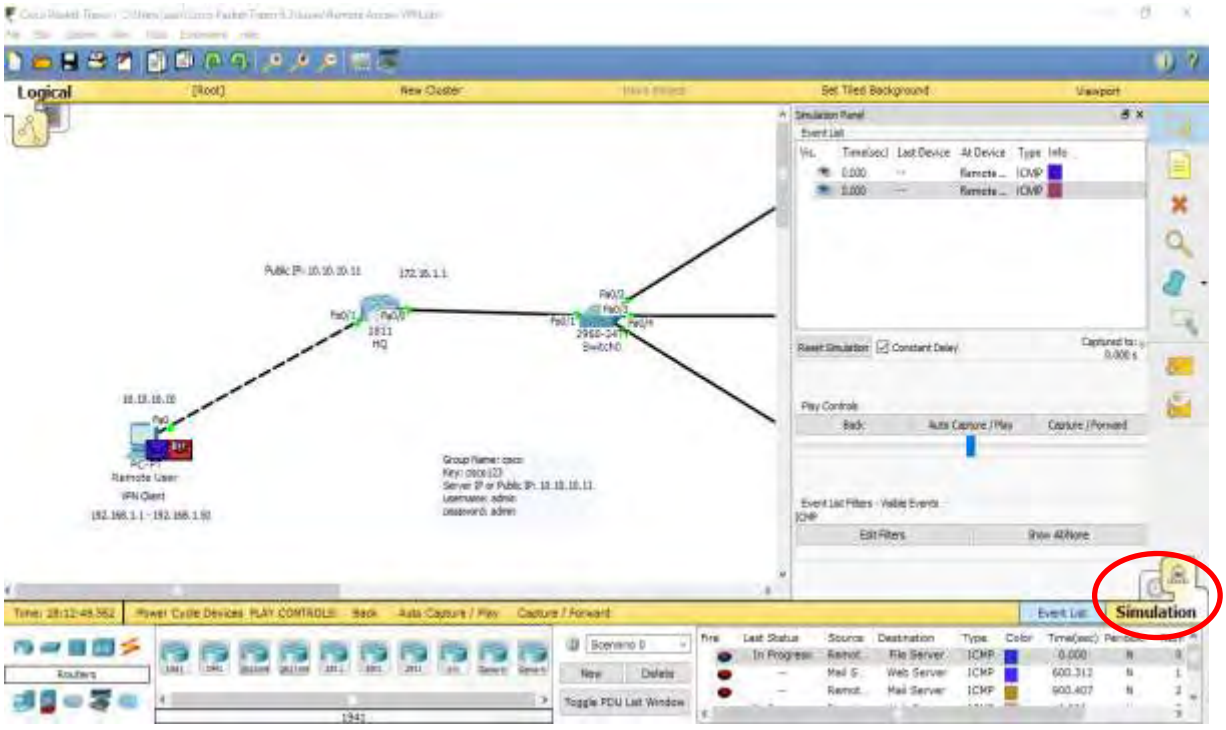


Εικόνα 32: Ip Remote User μετά τη σύνδεση στο VPN.



Εικόνα 33: Επικοινωνία του Remote User με τους Servers του δικτύου μέσω του VPN.

Τέλος, μπορούμε να ελέγξουμε την επικοινωνία μεταξύ των ενδιαφερόμενων άκρων στέλνοντας πακέτα PDU – μια δυνατότητα που μας δίνει το cisco packet tracer. Για να ξεκινήσουμε την προσομοίωση των πακέτων πρέπει να ξεκινήσουμε το Simulation στο packet tracer (Εικόνα 34).



Εικόνα 34: Cisco Packet Tracer Simulation.

Ανοίγει το παράθυρο της προσομοίωσης και επιλέγουμε Show All/None. Στη συνέχεια επιλέγω Edit Filters και διαλέγουμε ICMP. Επιλέγουμε το πακέτο και το τοποθετούμε στα δυο άκρα μεταξύ των οποίων θέλω να γίνει η ανταλλαγή δεδομένων. Επιλέγουμε auto capture/Play και βλέπουμε στην προσομοίωση τη μεταφορά των πακέτων. Υπάρχει η δυνατότητα αποστολής και δύο πακέτων ταυτόχρονα από το Remote User στους Servers.

Ο συνολικός προγραμματισμός του cisco router παρουσιάζεται στο Παράρτημα Α. Το συνολικό configuration μπορούμε να το δούμε μέσω της εντολής HQ#**show running-config.**

5.3 Προσομοίωση 2: Σύνδεση απομακρυσμένου χρήστη μέσω VPN στο δίκτυο μιας εταιρίας.

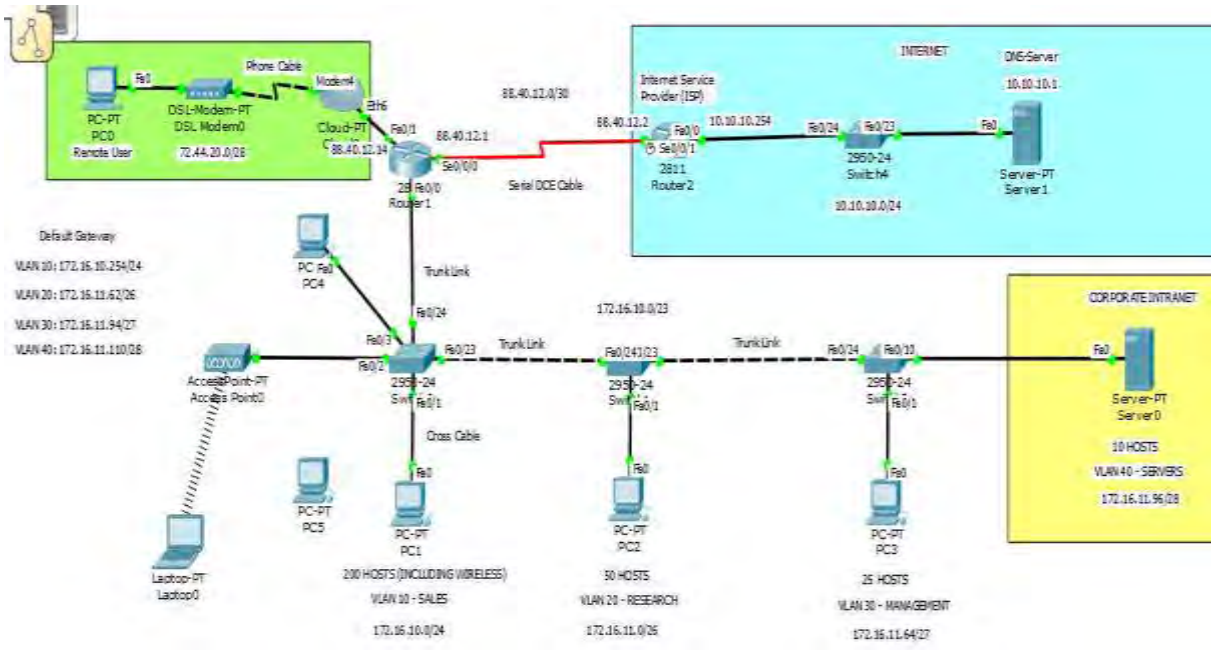
Σκοπός της προσομοίωσης αυτής είναι η παρουσίαση μιας πιο σύνθετης προσομοίωσης, όπου θα παρουσιάσουμε ένα **πραγματικό δίκτυο μιας εταιρίας** με δυο servers (internet & intranet), δύο router, τέσσερα switches, ένα access point και έναν απομακρυσμένο χρήστη (Remote User) ο οποίος θα συνδεθεί μέσω ίντερνετ στο δίκτυο της εταιρίας. Με τον τρόπο αυτό επιλέξαμε εκτός από την ασφάλεια που προσφέρει το VPN να εστιάσουμε και στην ευκολία ενός χρήστης που μπορεί να βρίσκεται πολλά χιλιόμετρα μακριά από την εταιρία να συνδεθεί στο δίκτυό της και να δουλέψει απομακρυσμένα.

Όμως, γιατί είναι σημαντικό να χρησιμοποιήσουμε remote πρόσβαση ενός χρήστη σε ένα vpn; Είναι σημαντικό γιατί δίνει τη δυνατότητα σε ένα απομακρυσμένο χρήστη να έχει πρόσβαση σε ένα

ιδιωτικό δίκτυο πάνω από το ίντερνετ με ασφάλεια χωρίς να περνάει από το κοινόχρηστο δίκτυο του ίντερνετ με το traffic αλλά από ένα συγκεκριμένο δρόμο – μονοπάτι – tunnel.

Η προσομοίωση, όπως αναφέρθηκε και στην προηγούμενη προσομοίωση, πραγματοποιήθηκε με τη χρήση του λογισμικού **Cisco Packet Tracer** (version 6.3).

Στην παρακάτω εικόνα παρουσιάζεται η συνολική εικόνα του δικτύου μας.



Εικόνα 35: Σύνδεση απομακρυσμένου χρήστη μέσω VPN στο δίκτυο μιας εταιρίας.

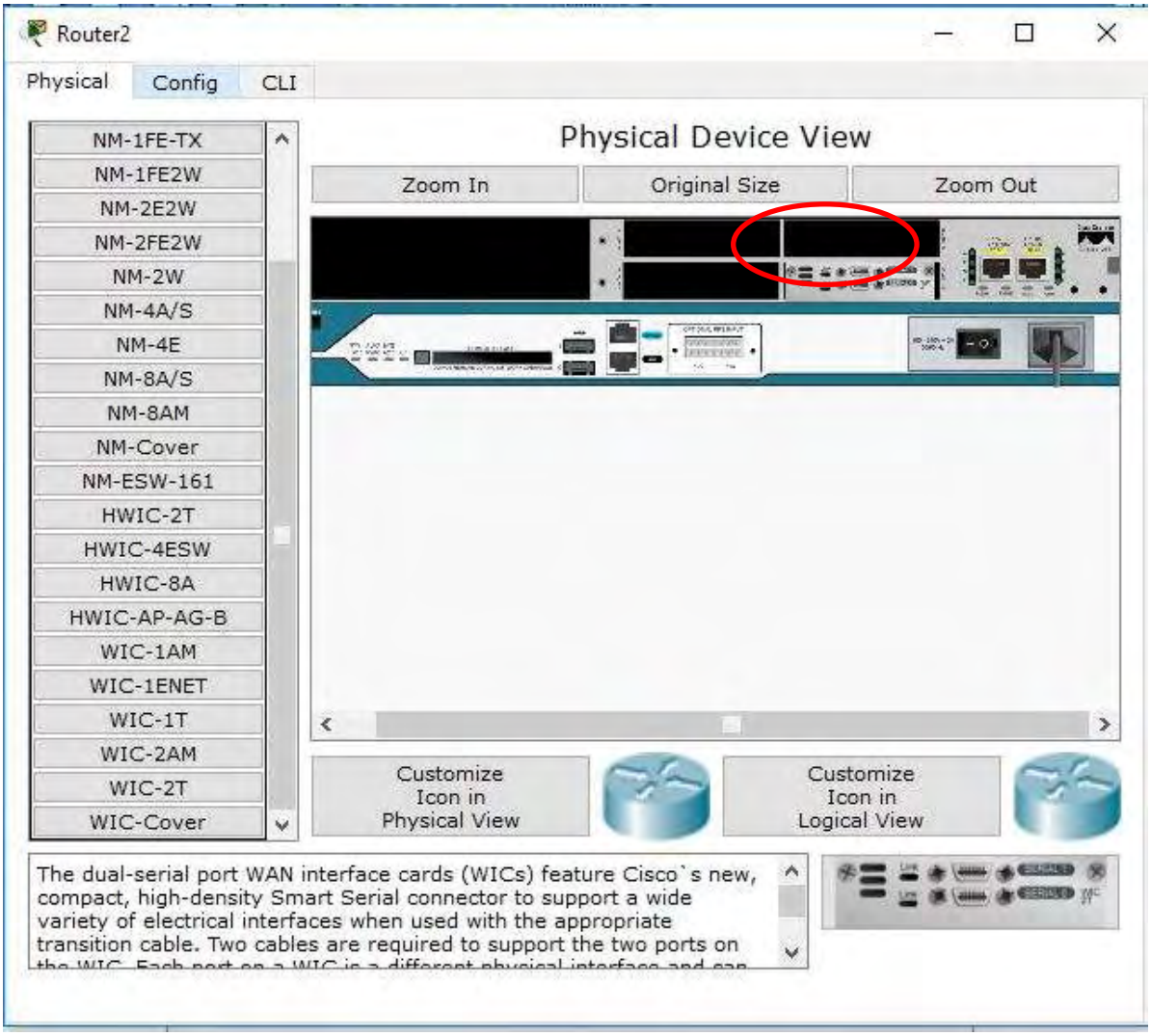
Στην προσομοίωση χρησιμοποιήσαμε δύο Cisco Router 2811, τέσσερα Switches 2950-24, δύο Servers (έναν για το Internet της εταιρίας και έναν για το Intranet), ένα access point για σύνδεση χρηστών με wireless μέσα στο δίκτυο και τέλος ένα DSL Modem για να συνδέσουμε μέσω Internet στο VPN το Remote χρήστη. Προκειμένου να λειτουργήσει σωστά ένα δίκτυο, πρέπει εκτός από τον κατάλληλο εξοπλισμό – ο οποίος θα προγραμματιστεί σωστά, να κάνουμε και τις απαραίτητες συνδέσεις μεταξύ τους. Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά όλες οι συνδέσεις που έγιναν μεταξύ των συσκευών του δικτύου.

Αφετηρία		**Τερματισμός**		**Τύπος Καλωδίου**
Συσκευή	**Προφίλ**	**Συσκευή**	**Προφίλ**	
Cisco Router 1	serial 0/0/0	Cisco Router 2	serial 0/0/1	Serial DCE cable
Cisco Router 2	Fa0/0	Switch 4 (SW4)	Fa0/24	Copper straight-through
Switch 4 (SW4)	Fa0/23	Server 1	Fa0	Copper straight-through
Switch 0 (SW1)	Fa0/2	Access Point	Port0	Copper straight-through
Switch 0 (SW1)	Fa0/24	Cisco Router 1	Fa0/0	Copper straight-through

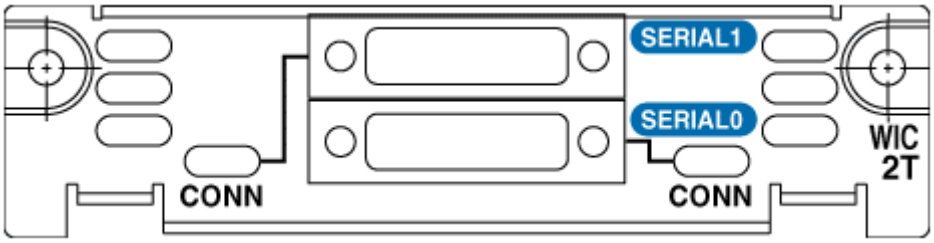
Switch 0 (SW1)	Fa0/23	Switch 1 (SW2)	Fa0/24	Copper Cross-Over
Switch 0 (SW1)	Fa0/1	PC 1	Fa0	Copper straight-through
Switch 1 (SW2)	Fa0/1	PC 2	Fa0	Copper straight-through
Switch 1 (SW2)	Fa0/23	Switch 2 (SW3)	Fa0/24	Copper Cross-Over
Switch 2 (SW3)	Fa0/1	PC 3	Fa0	Copper straight-through
Switch 2 (SW3)	Fa0/10	Server 0	Fa0	Copper straight-through

Εικόνα 36: Συνδεσμολογία Δικτύου 2.

Έχουμε τοποθετήσει δυο cisco routers 2811, όπως φαίνεται παραπάνω. Στον καθένα τοποθετούμε μια επιπλέον κάρτα ως εξής: απενεργοποιώ τη συσκευή, επιλεγώ από την αριστερή λίστα WIC-2T (dual serial port WAN interface) και σέρνω το εικονίδιο με την κάρτα στην κενή θέση (εικόνα 37).



Εικόνα 37: Dual serial port WAN interface cisco router



Εικόνα 38: Κάρτα dual serial port WAN

Την παραπάνω κάρτα την τοποθετούμε προκειμένου να έχουμε **δύο επιπλέον σειριακές συνδέσεις**. Χρησιμοποιήσαμε τη μια εκ των δύο στη σύνδεση μεταξύ των δύο cisco router (serial 0/0/0 & serial 0/0/1).

Στο σημείο αυτό θα πρέπει να αναφέρουμε μερικά χαρακτηριστικά των switches. Το switch είναι μια συσκευή η οποία φιλτράρει και προωθεί ένα πακέτο δεδομένων μεταξύ των τμημάτων ενός δικτύου. Τα Switches λειτουργούν στο data link layer (layer 2) και μερικές φορές στο network layer (layer 3) του μοντέλου OSI Reference Model, υποστηρίζοντας κάθε είδους πρωτόκολλο. Τα δίκτυα που χρησιμοποιούν switches για την επικοινωνία των τμημάτων τους καλούνται switched LANs ή στην περίπτωση των δικτύων Ethernet, switched Ethernet LANs**.**

Όταν σε ένα τμήμα Ethernet υπάρχουν περισσότεροι από ένας χρήστες, πράγμα που είναι το πιθανότερο, το αναπόφευκτο αποτέλεσμα είναι ο ανταγωνισμός μέσων (contention) και οι συγκρούσεις. Οι συγκρούσεις δημιουργούνται όταν δύο συσκευές προσπαθούν να στείλουν ταυτόχρονα δεδομένα στο κοινόχρηστο τμήμα (περιοχή εκπομπής). Επίσης, το γεγονός ότι στο HUB κάθε πακέτο αναμεταδίδετε σε κάθε πόρτα αυτό δημιουργεί ένα καταιγισμό πακέτων και υπερβολική κίνηση στο δίκτυο.

Το switch λύνει αρκετά από τα παραπάνω προβλήματα με τους εξής τρόπους. Ο διαχωρισμός των περιοχών εκπομπής σε μικρότερες (εικονικά LAN) VLAN, εξαλείφει το πρόβλημα του ανταγωνισμού και τον συγκρούσεων. Αυτή τη μέθοδο θα εφαρμόσουμε και εμείς στην προσομοίωσή μας, όπως θα δούμε παρακάτω.

Επίσης, η δυνατότητα εκμάθησης MAC διευθύνσεων και οι καταγραφή αυτών σε πίνακα δεδομένων σταματά το πρόβλημα του καταιγισμού. Για παράδειγμα, εάν σε ένα δίκτυο με 10 υπολογιστές ο Η/Υ Νο 2 θέλει να επικοινωνήσει με τον Νο 6 ένα HUB θα μετέδιδε τα πακέτα του 2 σε όλες τις πόρτες του με αποτέλεσμα να δημιουργηθεί καταιγισμός πακέτων. Ένα switch όμως έχοντας καταγεγραμμένο σε ποια πόρτα του, βρίσκετε ο Η/Υ 6 (καταγράφετε στην ουσία η MAC ADDRESS του Η/Υ 6) τότε το πακέτο από τον Η/Υ 2 θα αναμεταδοθεί μόνο στην πόρτα που βρίσκεται ο Η/Υ 6, χωρίς να κατακλυστούν οι Η/Υ όλου του δικτύου με πακέτα (καταιγισμός). Επίσης το switch έχει τη δυνατότητα περιορισμών (SECURITY) σε κάθε πόρτα του, έτσι ώστε να μπορεί να υποχρεώνει τον χρήστη να συνδέει έναν Η/Υ με μια συγκεκριμένη MAC ADDRESS σε μία και μοναδική πόρτα του switch που μόνο εκεί θα μπορεί να λειτουργεί. Περιορισμός MAC διευθύνσεων για μια συγκεκριμένη θύρα και άλλα.

Όπως αναφέραμε και πιο πάνω, στα τοπικά δίκτυα, μία στοιχειώδης έννοια είναι η περιοχή καθολικής εκπομπής (**broadcast domain**), η οποία ορίζεται ως το σύνολο των διασυνδεδεμένων κόμβων που μπορούν να λάβουν το πλαίσιο καθολικής εκπομπής του δικτύου (δηλαδή, για την

περίπτωση των δικτύων Ethernet, που μπορούν να λάβουν το πλαίσιο με διεύθυνση προορισμού την ffff.ffff.ffff).

Το ιδεατό τοπικό δίκτυο (virtual LAN – VLAN) έρχεται να καλύψει την ανάγκη δημιουργίας πολλαπλών και ανεξάρτητων περιοχών καθολικής εκπομπής μεταξύ υπολογιστών, ανεξάρτητα από τη φυσική τους τοποθέτηση. Δηλαδή, πάνω στο ίδιο μέσο πολλαπλής πρόσβασης μπορούν να δημιουργηθούν πολλά VLANs ή ένα VLAN μπορεί να υπάρξει μεταξύ υπολογιστών που διασυνδέονται σε ανεξάρτητα και απομακρυσμένα φυσικά μέσα.

Με τη δημιουργία **VLANs επιτυγχάνουμε την ομαδοποίηση των χρηστών σε ομοειδή λειτουργικά σύνολα,** ανεξάρτητα από το που βρίσκονται οι υπολογιστές τους. Το σημαντικό όφελος από αυτό το διαχωρισμό είναι η αυξημένη προστασία από κακόβουλη ή εσφαλμένη χρήση του δικτύου. Η σύσταση ενός VLAN πραγματοποιείται διαμέσου του λογισμικού των δικτυακών συσκευών. Έτσι, είναι πολύ εύκολη η ανασύστασή του σε περιπτώσεις όπου π.χ. αλλάζει γραφείο ένας υπάλληλος ή προστίθεται ένα νέο μέλος σε μία ομάδα.

Το VTP (VLAN Trunking Protocol) είναι ένα πρωτόκολλο μηνυμάτων Layer 2 που χρησιμοποιείται για τη διανομή και το συγχρονισμό πληροφοριών αναγνώρισης VLAN τα οποία είναι διευθετημένα σε ένα δίκτυο μεταγωγής. Οι ρυθμίσεις που γίνονται σε ένα SWITCH σε κατάσταση VTP Server διαδίδονται μέσω αυτού σε όλους τους συνδεδεμένους μεταγωγείς του δικτύου περιορίζοντας την ανάγκη διευθέτησης των δικτύων με το χέρι. Δηλαδή, το vtp είναι ένα πρωτόκολλο που χρησιμοποιείται μεταξύ των μεταγωγέων για τη διαχείριση των VLANs. Θα το χρησιμοποιήσουμε και στην προσομοίωσή μας.

Trunking και access port

Μία access port επιτρέπει μονάχα frames που είναι tagged με το συγκεκριμένο VLAN ID στο οποίο ανήκει η πόρτα. Μία trunk από την άλλη, επιτρέπει tagged frames που έχουν οποιοδήποτε_VLAN-ID. Γενικά, μία **access port** εξυπηρετεί κάποιον **host του δικτύου**, ενώ μία **trunk** εξυπηρετεί ένα **uplink** σε κάποιο άλλο **switch** ή ένα **inter-VLAN routing interface**. Έτσι λοιπόν και στη δική μας προσομοίωση έχουμε προγραμματίσει τις πόρτες που συνδέουν τα switch μεταξύ τους ως trunk. Την αναλυτική παραμετροποίηση θα τη βλέπουμε στον παρακάτω πίνακα.

Συσκευή: Switch 0 (από εδώ και στο εξής το ονομάζω SW1)	
Εντολή	**Περιγραφή**
Switch>**enable**	Εισαγωγή σε privilege mode, όπου μπορούμε να δούμε όλα τα configurations που έχουνε γίνει στο Switch αλλά και να το προγραμματίσουμε.
Switch#**configure terminal**	Εισαγωγή σε Global Configuration Mode, όπου γίνεται ο προγραμματισμός του Switch.
Switch (config)#**hostname SW1**	Δίνουμε όνομα στο Switch (Στην περίπτωσή μας το ονομάζουμε

	SW1).
SW1(config)#**interface range fastEthernet 0/23 - 24**	Ρύθμιση του εύρους του fast ethernet interface. Δηλαδή, θα προγραμματίσουμε ταυτόχρονα το προφίλ fastEthernet 0/23 και fastEthernet 0/24.
SW1(config-if-range)#**switchport mode trunk**	Ορίζω τα δύο παραπάνω προφίλ στα οποία έχω συνδέσει το Router 1 και το Switch 1 αντίστοιχα ως trunk πόρτες.
SW1#**wr**	Αποθηκεύει το configuration και πιο συγκεκριμένα αντιγράφει το running-config (παραμετροποίηση που έχει γίνει στη μνήμη RAM) στο startup-config (παραμετροποίηση που θα εφαρμοστεί αν σβήσει και ανάψει εκ νέου το switch).
SW1(config)#**vtp mode server**	Το πρωτόκολλο VLAN Trunking Protocol (VTP) έχει τρείς διαφορετικές μορφές: server, client, transparent. Επιλέχθηκε το πρώτο.
SW1(config)#**vtp domain CISCO**	Ορίζω το όνομα του vtp domain.
SW1(config)#**vtp password ov**	Ορίζω τον κωδικό πρόσβασης στο vtp domain.
SW1(config)#**vlan 10**	Αρχίζω να διαμορφώνω τα vlans. Το πρώτο θα είναι το vlan νούμερο 10.
SW1(config-vlan)#**name SALES**	Και θα έχει όνομα “SALES”.
SW1(config-vlan)#**exit**	Βγαίνω από την παραμετροποίηση του VLAN.
SW1(config)#**vlan 20**	Το δεύτερο θα είναι το vlan νούμερο 20.
SW1(config-vlan)#**name RESEARCH**	Και θα έχει όνομα “RESEARCH”.
SW1(config-vlan)#**exit**	Βγαίνω από την παραμετροποίηση του VLAN.
SW1(config)#**vlan 30**	Το τρίτο θα είναι το vlan νούμερο 30.

SW1(config-vlan)#**name MANAGEMENT**	Και θα έχει όνομα “MANAGEMENT”.
SW1(config-vlan)#**exit**	Βγαίνω από την παραμετροποίηση του VLANs.
SW1(config)#**vlan 40**	Το τέταρτο θα είναι το vlan νούμερο 40.
SW1(config-vlan)#**name SERVERS**	Και θα έχει όνομα “SERVERS”.
SW1(config)#**interface range fastEthernet 0/1 - 20**	Ρύθμιση του εύρους του fast ethernet interface. Δηλαδή, θα προγραμματίσουμε ταυτόχρονα τα προφίλ fastEthernet 0/1 έως fastEthernet 0/20.
SW1(config-if-range)#**switchport mode access**	Ορίζω όλες τις πόρτες να είναι access.
SW1(config-if-range)#**switchport access vlan 10**	Ορίζω όλες τις πόρτες που είναι access στο vlan 10

Πίνακας 6: Παραμετροποίηση του Switch - Δίκτυο 2.

Άρα ο παραπάνω πίνακας μας δείχνει αναλυτικά τον τρόπο που έγινε η παραμετροποίηση του πρώτου switch. Οι παρακάτω εντολές εάν εφαρμοστούν στο switch μας δείχνουν όλα τα παραπάνω:

```
SW1#show vtp status
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9 //είχαμε 5 default VLANs και με τα 4 καινούρια που προσθέσαμε, έχουμε σύνολο 9
VTP Operating Mode              : Server
VTP Domain Name                 : CISCO
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDF 0x31 0xAC 0x92 0x85 0xF9 0x74 0xCB
Configuration last modified by 0.0.0.0 at 3-1-93 01:34:20
Local updater ID is 0.0.0.0 (no valid interface found)
SW1#
SW1#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/21, Fa0/22
```

10 SALES active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
20 RESEARCH active
30 MANAGEMENT active
40 SERVERS active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

Όμοια, προγραμματίζω και για τα άλλα switches. Άρα πάω στο switch 1 (από εδώ και στο εξής το ονομάζω SW2) και στο switch 2 (από εδώ και στο εξής το ονομάζω SW3) και το παραμετροποιώ ακριβώς όπως το πρώτο. Βλέπουμε ότι τα αντίστοιχα interfaces που πρέπει να γίνουν trunk στο SW2 είναι Fa0/23 & Fa0/24 και στο SW3 το Fa0/24.

Το μόνο που αλλάξω κάθε φορά είναι σε ποιο VLAN θέτω τις access ports. Βλέπουμε και στο σχήμα του δικτύου ότι στο SW2 έχουμε access ports στο VLAN 20 – RESEARCH. Όμοια, στο SW3 έχουμε access ports στο VLAN 30 – MANAGEMENT και στο VLAN 40 - SERVERS. Όλες οι παραμετροποιήσεις του δικτύου 2 βρίσκονται στο Παράρτημα Β.

Στη συνέχεια, θα προγραμματίσουμε το cisco router 1 του δικτύου μας, το οποίο συνδέεται με το SW1 και το 2ο cisco router. Στο cisco router 1 θα συνδεθεί εν συνεχεία και ο απομακρυσμένος χρήστης.

Συσκευή: cisco router 1 (από εδώ και στο εξής το ονομάζω R1)	
Εντολή	**Περιγραφή**
Router>**enable**	Εισαγωγή σε privilege mode, όπου μπορούμε να δούμε όλα τα configurations που έχουνε γίνει στο Router αλλά και να το προγραμματίσουμε.
Router#**configure terminal**	Εισαγωγή σε Global Configuration Mode, όπου γίνεται ο προγραμματισμός του Router.
Router (config)#**hostname R1**	Δίνουμε όνομα στο Router (Στην περίπτωσή μας το ονομάζουμε R1).
R1(config)#**interface fastEthernet 0/0**	Ρύθμιση του fast ethernet interface 0/0. Προς την πλευρά αυτή έχουμε τη σύνδεση με το switch που είναι σε trunk mode.

R1(config-if)#**no ip address**	Άρα δεν πρέπει να ορίσουμε διεύθυνση IP προς την πλευρά αυτή.
R1(config-if)#**no shutdown**	Ενεργοποιεί το συγκεκριμένο interface.
R1(config)#**interface fastEthernet 0/0.10**	Στη συνέχεια, θα ορίσουμε τα interfaces των vlans. Ξεκινάω με το vlan 10.
R1(config-subif)#**encapsulation dot1Q 10**	Ενεργοποιεί το πρωτόκολλο IEEE 802.1Q στο vlan 10. Συνοπτικά, το πρωτόκολλο αυτό χωρίζει μεγάλα δίκτυα ή υποδίκτυα σε μικρότερα προκειμένου να διαχειρίζεται καλύτερο ο cisco router το traffic.
R1(config-subif)#**ip address 172.16.10.254 255.255.255.0**	Ορίζω τις διευθύνσεις για το vlan 10. Δηλαδή, ορίζω τη μέγιστη ip address & το subnet mask για το vlan 10.
R1(config-subif)#**exit**	Αποχωρώ από την παραμετροποίηση του vlan 10.
R1(config)#**interface fastEthernet 0/0.20**	Θα ορίσουμε το interface του vlan 20.
R1(config-subif)#**encapsulation dot1Q 20**	Ενεργοποιεί το πρωτόκολλο IEEE 802.1Q στο vlan 20.
R1(config-subif)#**ip address 172.16.11.62 255.255.255.192**	Ορίζω τις διευθύνσεις για το vlan 20. Δηλαδή, ορίζω τη μέγιστη ip address & το subnet mask για το vlan 20.
R1(config-subif)#**exit**	Αποχωρώ από την παραμετροποίηση του vlan 20.
R1(config)#**interface fastEthernet 0/0.30**	Θα ορίσουμε το interface του vlan 30.
R1(config-subif)#**encapsulation dot1Q 30**	Ενεργοποιεί το πρωτόκολλο IEEE 802.1Q στο vlan 30.
R1(config-subif)#**ip address 172.16.11.94 255.255.255.224**	Ορίζω τις διευθύνσεις για το vlan 30. Δηλαδή, ορίζω τη μέγιστη ip address & το subnet mask για το vlan 30.
R1(config-subif)#**exit**	Αποχωρώ από την παραμετροποίηση του vlan 30.
R1(config)#**interface fastEthernet 0/0.40**	Θα ορίσουμε το interface του vlan 40.

R1(config-subif)#**encapsulation dot1Q 40**	Ενεργοποιεί το πρωτόκολλο IEEE 802.1Q στο vlan 40.
R1(config-subif)#**ip address 172.16.11.110 255.255.255.224**	Ορίζω τις διευθύνσεις για το vlan 40. Δηλαδή, ορίζω τη μέγιστη ip address & το subnet mask για το vlan 40.
R1(config-subif)#**exit**	Και θα έχει όνομα “SERVERS”.

Πίνακας 7: Παραμετροποίηση του cisco router 1 - Δίκτυο 2 – μέρος 1.

Με την παρακάτω εντολή βλέπουμε την παραμετροποίηση των VLANS στο cisco router 1:

R1#**show ip int brief**
Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 unassigned YES unset up up

FastEthernet0/0.10 172.16.10.254 YES manual up up

FastEthernet0/0.20 172.16.11.62 YES manual up up

FastEthernet0/0.30 172.16.11.94 YES manual up up

FastEthernet0/0.40 172.16.11.110 YES manual up up

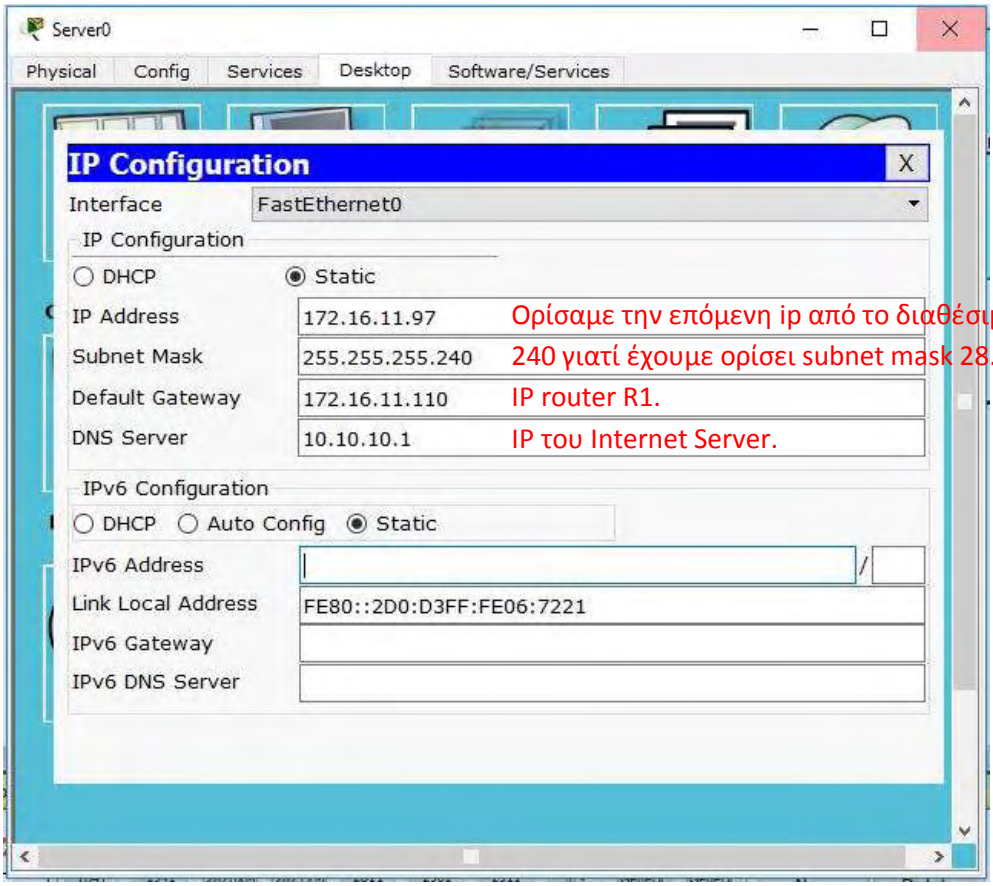
FastEthernet0/1 unassigned YES unset administratively down down

Serial0/0/0 unassigned YES unset administratively down down

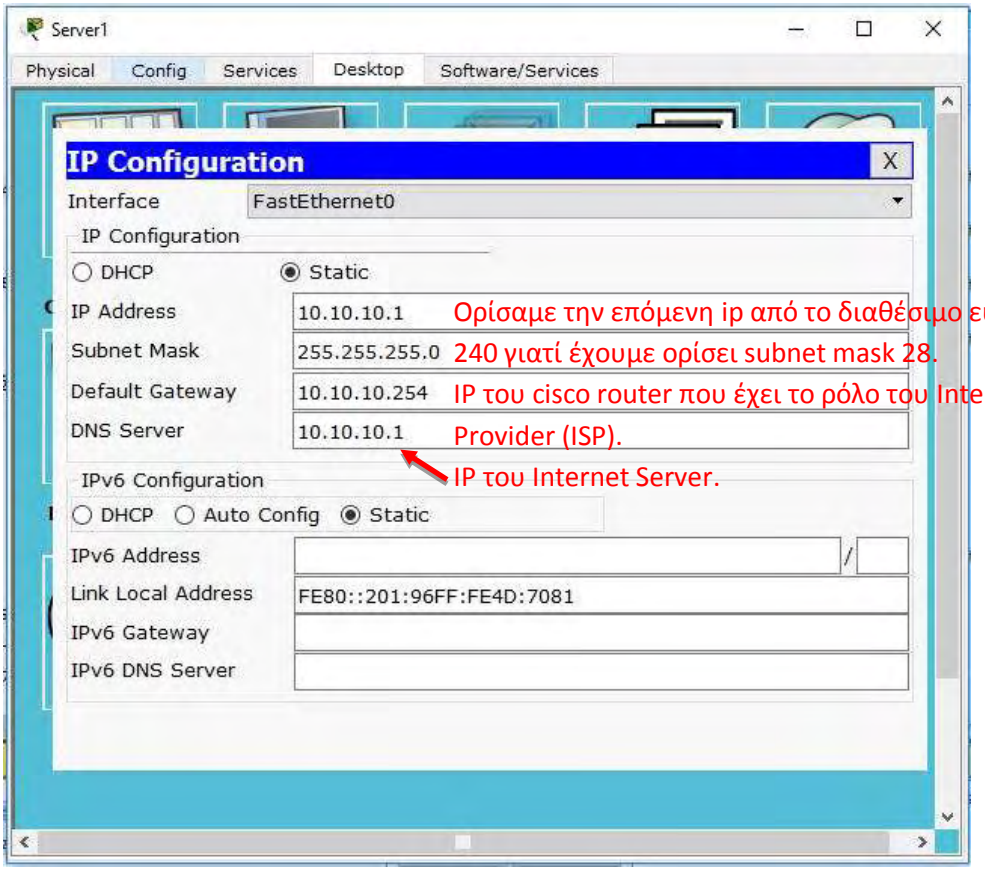
Serial0/0/1 unassigned YES unset administratively down down

Vlan1 unassigned YES unset administratively down down
R1#

Στη συνέχεια, παρουσιάζονται οι ips που ορίσαμε στους δύο Servers του δικτύου μας. Να επισημάνουμε ότι στο Server του Intranet, όπως και στο Server του Internet ορίσαμε static IP. Αναλυτικά φαίνονται στις παρακάτω εικόνες.



Εικόνα 39: IP Address Intranet Server.



Εικόνα 40: IP Address Internet Server.

Στη συνέχεια, θα ξεκινήσουμε την παραμετροποίηση του Internet Service Provider (ISP) cisco router 2. Στον πίνακα που ακολουθεί φαίνονται οι εντολές που δόθηκαν στο cisco router.

Συσκευή: cisco router 2 (από εδώ και στο εξής το ονομάζω ISP)	
Εντολή	**Περιγραφή**
Router>**enable**	Εισαγωγή σε privilege mode, όπου μπορούμε να δούμε όλα τα configurations που έχουνε γίνει στο Router αλλά και να το προγραμματίσουμε.
Router#**configure terminal**	Εισαγωγή σε Global Configuration Mode, όπου γίνεται ο προγραμματισμός του Router.
Router (config)#**hostname ISP**	Δίνουμε όνομα στο Router (Στην περίπτωσή μας το ονομάζουμε ISP).
ISP (config)#**interface fastEthernet 0/0**	Ρύθμιση του fast ethernet interface 0/0. Προς την πλευρά αυτή έχουμε τη σύνδεση με το switch 4 και κατ' επέκταση με τον Internet Server.
ISP(config-if)#**ip address 10.10.10.254 255.255.255.0**	Ορίζουμε τη διεύθυνση IP προς την πλευρά αυτή, καθώς και το subnet mask.
ISP (config-if)#**no shutdown**	Ενεργοποιεί το συγκεκριμένο interface.
ISP(config-if)#**exit**	Έξοδος από το συγκεκριμένο interface.
ISP(config)#**interface serial 0/0/1**	Ρύθμιση του προφίλ interface serial 0/0/1. Προς την πλευρά αυτή έχουμε τη σύνδεση με το cisco router 1.
ISP(config)#**ip route 172.16.10.0 255.255.254.0 88.40.12.1**	Ορίζουμε το routing table για να μπορούν πακέτα από το Server 1 να πηγαίνουν προς το cisco router R1 και κατ' επέκταση προς το υπόλοιπο δίκτυο. 172.16.10.0 είναι η βασική ip που «τμηματοποιήσαμε» για να φτιάξουμε τα υποδικτυα. 255.255.254.0 είναι το subnet mask (172.16.10.0/23).
ISP(config-if)#**ip address 88.40.12.2 255.255.255.252**	Ορίζουμε τη διεύθυνση IP προς την πλευρά αυτή, καθώς και το subnet mask.

ISP(config-if)#**clock rate 128000**	Η εντολή αυτή εφαρμόζεται μόνο σε DTE interface, όπως είναι αυτό που έχουμε προς την πλευρά αυτή. Ορίζει την ταχύτητα του link, δηλαδή την ταχύτητα επικοινωνίας ανάμεσα στα δύο cisco router. Επιλέξαμε 128000 bits per second. (Εξαρτάται από τις δυνατότητες της γραμμής Internet που διαθέτουμε.)
ISP(config-if)#**bandwidth 128**	Ορίζει ότι και η προηγούμενη εντολή (clock rate), αλλα μετριέται σε kbits per sec για αυτό το λόγο επιλέξαμε 128. Να επισημάνουμε ότι αυτές οι δύο εντολές είναι χρήσιμές για τα routing protocols δηλαδή για τα δεδομένα που αναταράσσονται μεταξύ των routers. Οπότε τους καθορίζω ουσιαστικά την ταχύτητα με την οποία θα ανταλλάσσουν δεδομένα μεταξύ τους.
ISP(config-if)#**no shutdown**	Ενεργοποιεί το συγκεκριμένο interface.

Πίνακας 8: Παραμετροποίηση του cisco router 2 - Δίκτυο 2 – μέρος 1.

Μπορούμε να δούμε όπως και πριν τα interface που δημιουργήσαμε με την παρακάτω εντολή:

SP#**show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.10.10.254	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	82.40.12.2	YES	manual	down	down
Vlan1	unassigned	YES	unset	administratively down	down

Επιστρέφουμε στην παραμετροποίηση του cisco router R1:

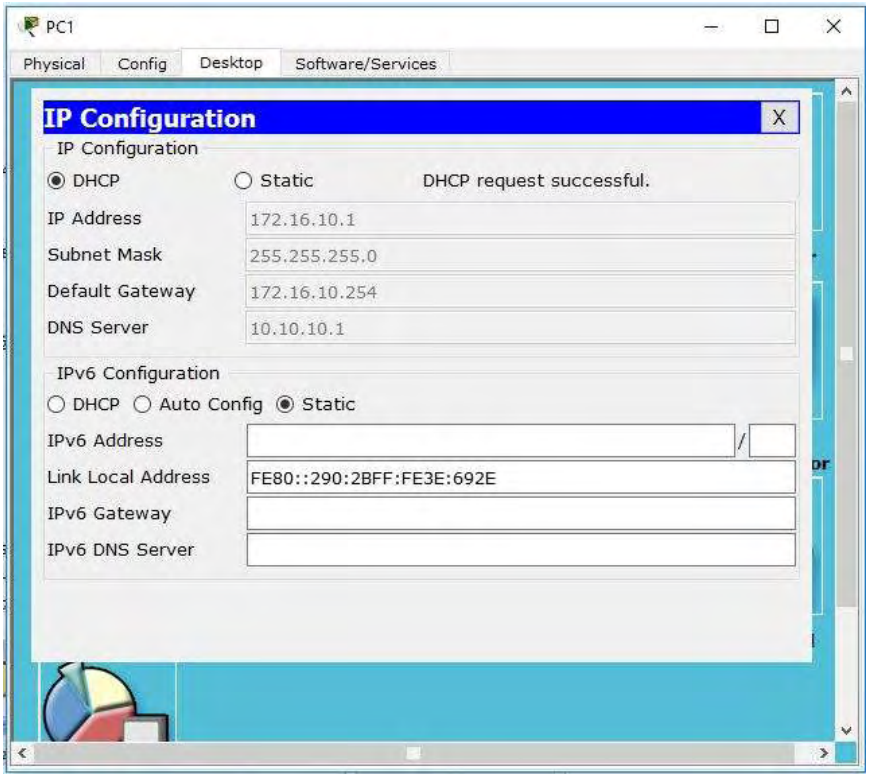
Συσκευή: cisco router 1 (R1)	
Εντολή	**Περιγραφή**
R1(config)#**interface s0/0/0**	Ξεκινάμε με τη παραμετροποίηση του serial interface s0/0/0.
R1(config-if)#**ip address 88.40.12.1 255.255.255.252**	Ορίζουμε την IP και το subnet mask.
R1(config-if)#**bandwidth 128**	Εδώ δεν έχουμε service provider end άρα δεν χρειαζόμαστε clock rate. Χρειαζόμαστε όμως το bandwith για να συγχρονίσουν τα πρωτοκόλλα. Ορίζω την ίδια ταχύτητα με πριν. (Όλα τα routing protocols χρειάζονται bandwith.)

R1(config-if)#**no shutdown**	Ενεργοποίηση του serial interface s0/0/0.
R1(config)#**ip route 0.0.0.0 0.0.0.0 serial 0/0/0**	Παραμετροποίηση του routing table για να μπορούν οι χρήστες να έχουν πρόσβαση στον Internet Server. Τα 0 σημαίνουν ότι οποιαδήποτε διεύθυνση ip του δικτύου να μπορεί να έχει πρόσβαση στην πλευρά του serial 0/0/0, δηλαδή στο internet.
R1(config)#**ip dhcp pool VLAN10**	Ορίζουμε δυναμικές ips σε όλους τους χρήστες - pcs που συνδέονται σε κάθε vlan. Ξεκινάμε με το vlan 10.
R1(dhcp-config)#**network 172.16.10.0 255.255.255.0**	Ορίζουμε τις διαθέσιμες IPs και subnet mask στους χρήστες που θα συνδεθούν στο vlan 10.
R1(dhcp-config)#**default-router 172.16.10.254**	Ορίζουμε το Default Router στο vlan1 0.
R1(dhcp-config)#**dns-server 10.10.10.1**	Ορίζουμε το Dns Server στο vlan 10.
R1(dhcp-config)#**exit**	Έξοδος από την παραμετροποίηση του vlan 10.
R1(config)#**ip dhcp pool VLAN20**	Ορίζουμε δυναμικές ips σε όλους τους χρήστες - pcs που συνδέονται στο vlan 20.
R1(dhcp-config)#**network 172.16.11.0 255.255.255.192**	Ορίζουμε τις διαθέσιμες IPs και subnet mask στους χρήστες που θα συνδεθούν στο vlan 20.
R1(dhcp-config)#**default-router 172.16.11.62**	Ορίζουμε το Default Router στο vlan 20.
R1(dhcp-config)#**dns-server 10.10.10.1**	Ορίζουμε το Dns Server στο vlan 20.
R1(dhcp-config)#**exit**	Έξοδος από την παραμετροποίηση του vlan 20.
R1(config)#**ip dhcp pool VLAN30**	Ορίζουμε δυναμικές ips σε όλους τους χρήστες - pcs που συνδέονται στο vlan 30.
R1(dhcp-config)#**network 172.16.11.64 255.255.255.224**	Ορίζουμε τις διαθέσιμες IPs και subnet mask στους χρήστες που θα συνδεθούν στο vlan 30.

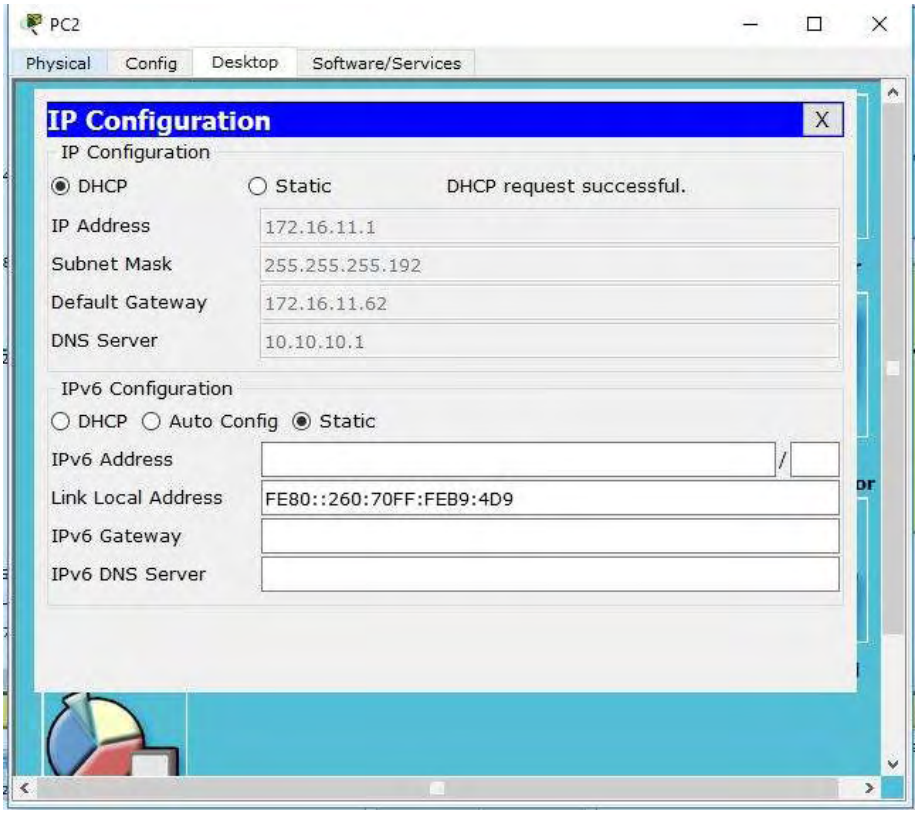
R1(dhcp-config)#**default-router 172.16.11.94**	Ορίζουμε το Default Router στο vlan 30.
R1(dhcp-config)#**dns-server 10.10.10.1**	Ορίζουμε το Dns Server στο vlan 30.
R1(dhcp-config)#**exit**	Έξοδος από την παραμετροποίηση του vlan 30.

Πίνακας 9: Παραμετροποίηση του cisco router 1 - Δίκτυο 2 – μέρος 2.

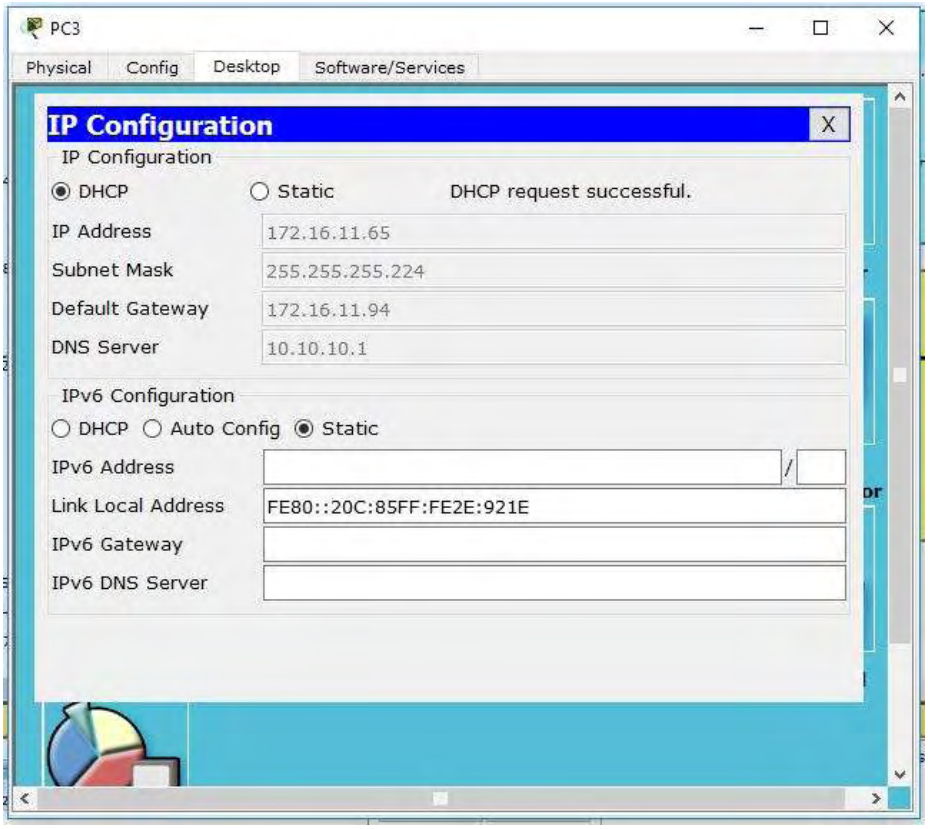
Άρα, πάω σε κάθε υπολογιστή και ορίζω dhcp (δυναμική) ip, όπως φαίνεται στις παρακάτω εικόνες.



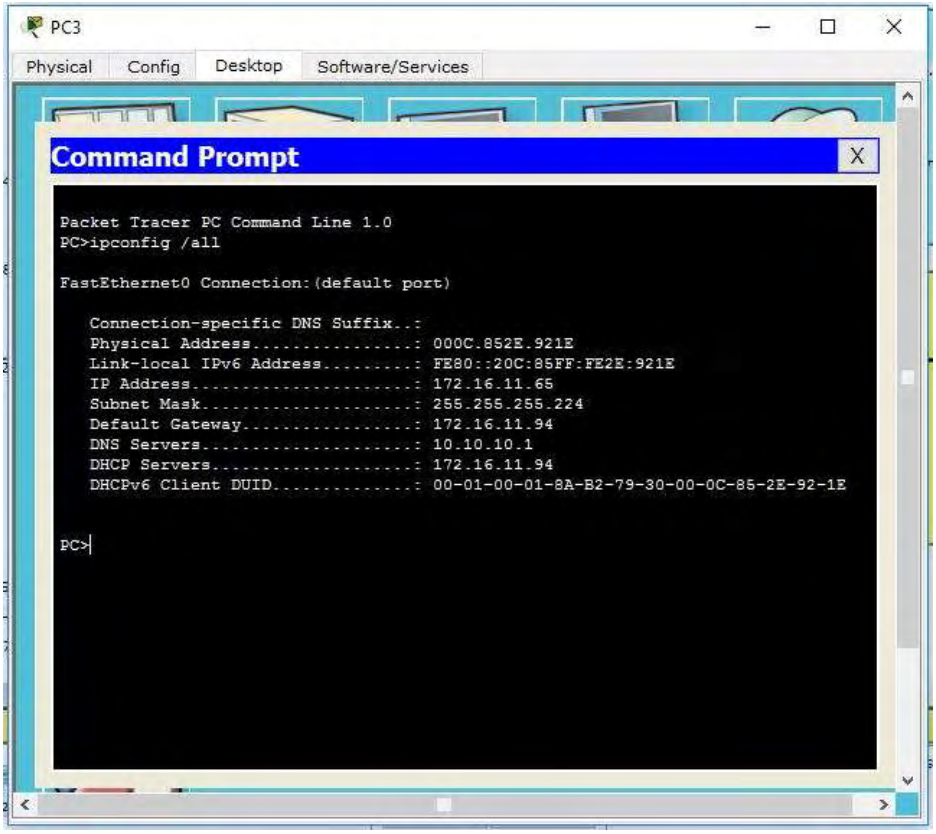
Εικόνα 41: Dhcp ip pc1.



Εικόνα 42: Dhcp ip pc2.



Εικόνα 43: Dhcp ip pc3.



Εικόνα 44: Ip Address από command prompt.

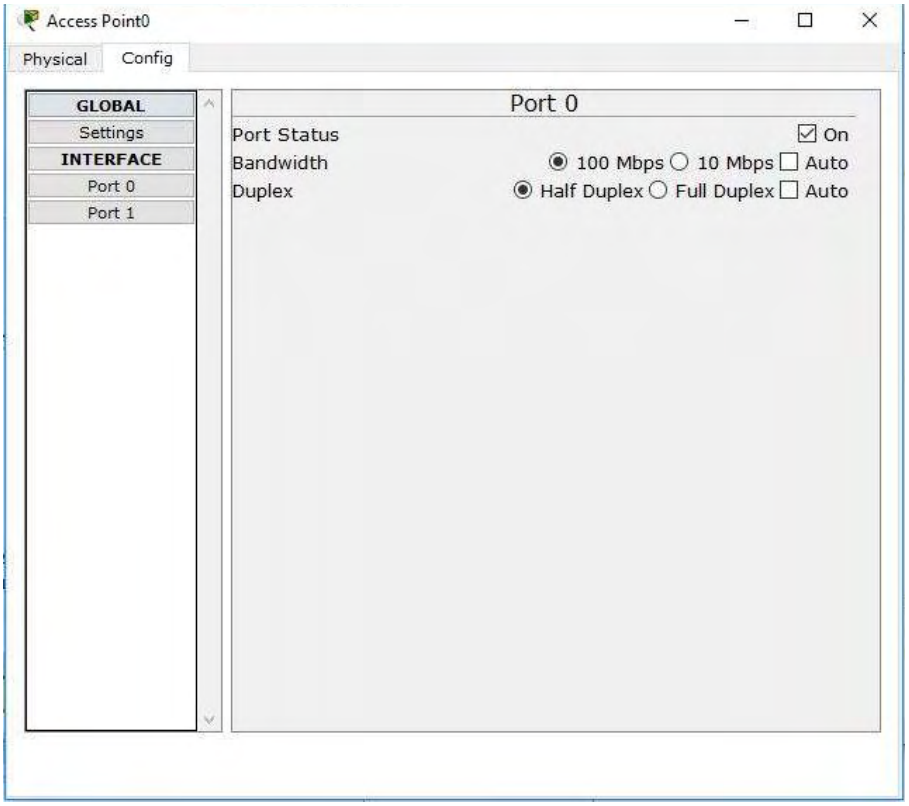
Στην εικόνα 44 φαίνεται μέσω της εντολής **ipconfig /all** στο command prompt του pc3 η διευθυνσιοδότηση του υπολογιστή αυτού, σύμφωνα με όσα ορίσαμε.

Μπορώ επίσης να δω από το router R1 την πρώτη ip address που μπορεί να πάρει κάθε υπολογιστής σε κάθε vlan.

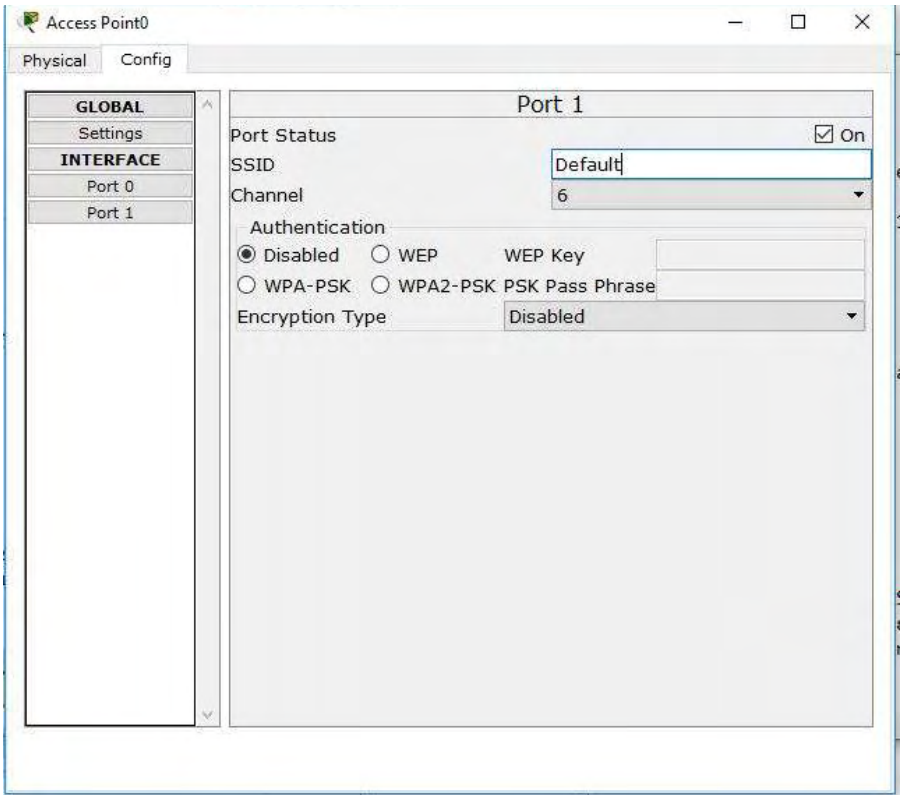
R1#**show ip dhcp binding**

IP address	Client-ID/ Hardware address	Lease expiration	Type	
172.16.10.1	0090.2B3E.692E	--	Automatic	//1η ip address sales
172.16.11.1	0060.70B9.04D9	--	Automatic	//1η ip address research
172.16.11.65	000C.852E.921E	--	Automatic	//1η ip address management

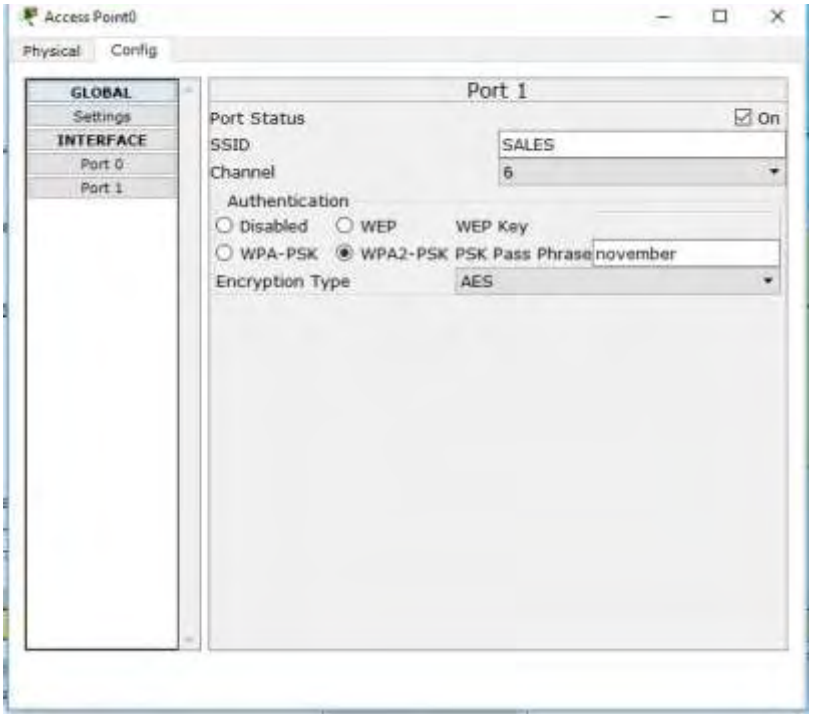
Θα προσθέσουμε ένα χρήστη που συνδέεται ασύρματα στο VLAN 10 – Sales. Για να το πετύχουμε αυτό πρέπει να χρησιμοποιήσουμε ένα Access Point. Το Access Point έχει δυο πόρτες. Την port0 & την port1. Η port0 χρησιμοποιείται ήδη για να το συνδέσουμε με το switch. Την port1 πρέπει να την προγραμματίσουμε. Στις παρακάτω εικόνες, παρουσιάζονται η αρχική και η τελική κατάσταση (μετά την παραμετροποίηση – port1) σε κάθε πόρτα του access point.



Εικόνα 45: Port0 access point.



Εικόνα 46: Port1 access point - πριν την παραμετροποίηση.



Εικόνα 47: Port1 access point - μετά την παραμετροποίηση.

Όπως φαίνεται στην παραπάνω εικόνα, ορίζουμε όνομα στο SSID → SALES. Το "authentication": WEP → δεν προσφέρει μεγάλη ασφάλεια και μπορεί κάποιος να σπάσει το κλειδί εύκολα. Άρα, χρησιμοποιούμε το WPA και πιο συγκεκριμένα το πιο ενισχυμένο WPA2-PSK. Ορίζουμε key → november και Encryption type → AES.

Άρα, στο σημείο αυτό, θα συνδέσουμε ένα laptop ασύρματα (wireless) με το VLAN 10 μέσω του access point. Ανοίγουμε το laptop και από την εικόνα του απενεργοποιώ την τροφοδοσία. Εάν θέλουμε, μπορούμε να του προσθέσουμε ένα module κατάλληλο για ασύρματη σύνδεση. Αφαιρούμε το προηγούμενο που είχε (WPC300N) και προσθέτουμε από την αριστερή λίστα το καινούριο (PT LAPTOP NM 1W). Ενεργοποιώ ξανά την τροφοδοσία.

Εικόνα 48: PT LAPTOP NM 1W module - Laptop.

Παραμετροποιούμε το laptop με τα στοιχεία που έχουμε ορίσει στο access point.

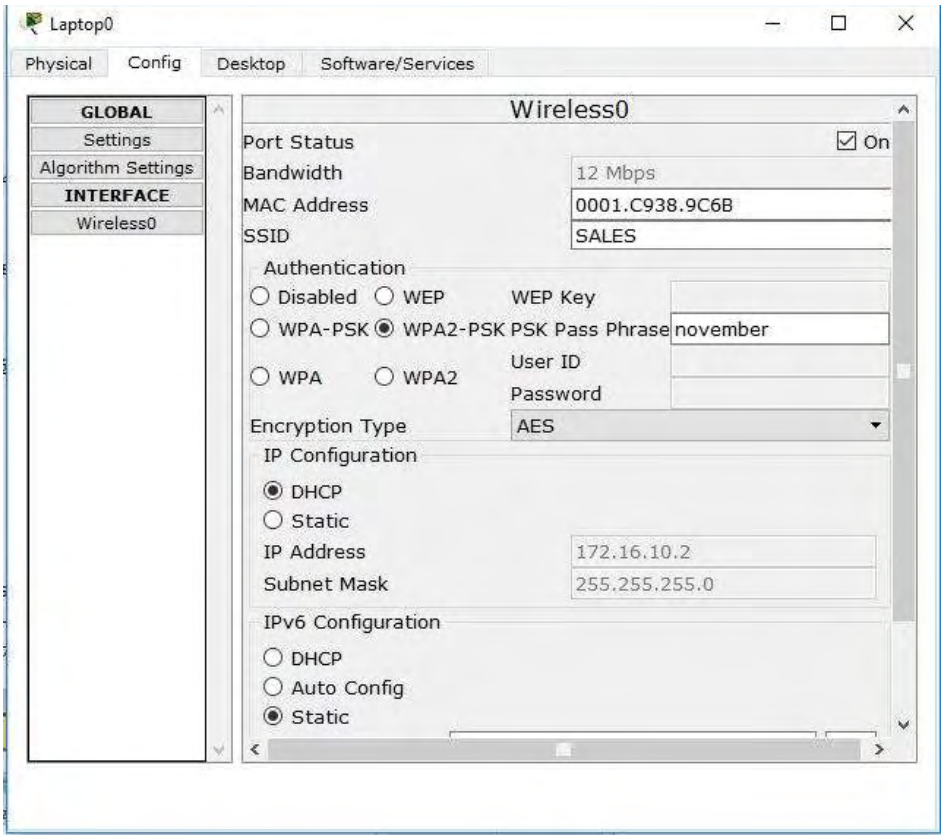
Laptop -> Config -> Wireless0:

SSID->SALES

authentication->WPA2-PSK

key -> November

Εννοείται ότι στο laptop, έχουμε ορίσει να παίρνει dhcp ip.



Εικόνα 49: Παραμετροποίηση του wireless στο laptop.

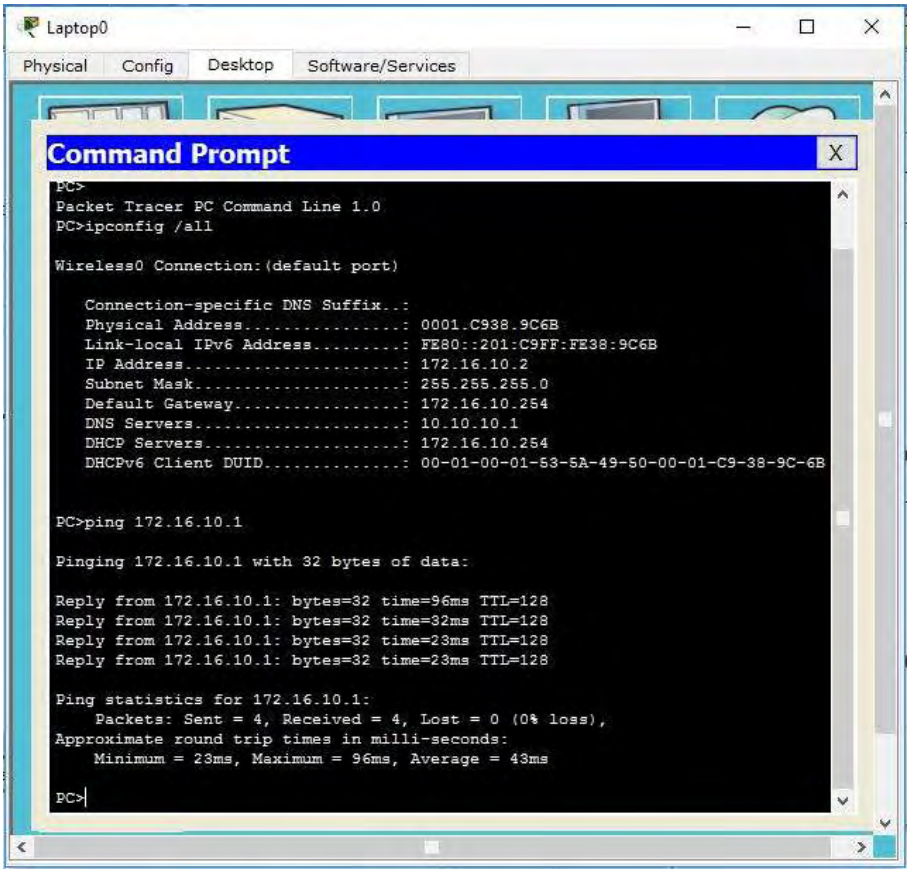
Άρα, εφαρμόζοντας εκ νέου στο router R1 το ίδιο command με πριν, παρατηρούμε ότι στο VLAN 10 έχει προστεθεί και μια δεύτερη ip address (172.16.10.2).

R1#**show ip dhcp binding**

IP address	Client-ID/ Hardware address	Lease expiration	Type	
172.16.10.1	0090.2B3E.692E	--	Automatic	
172.16.10.2	0001.C938.9C6B	--	Automatic	//laptop
172.16.11.1	0060.70B9.04D9	--	Automatic	
172.16.11.65	000C.852E.921E	--	Automatic	

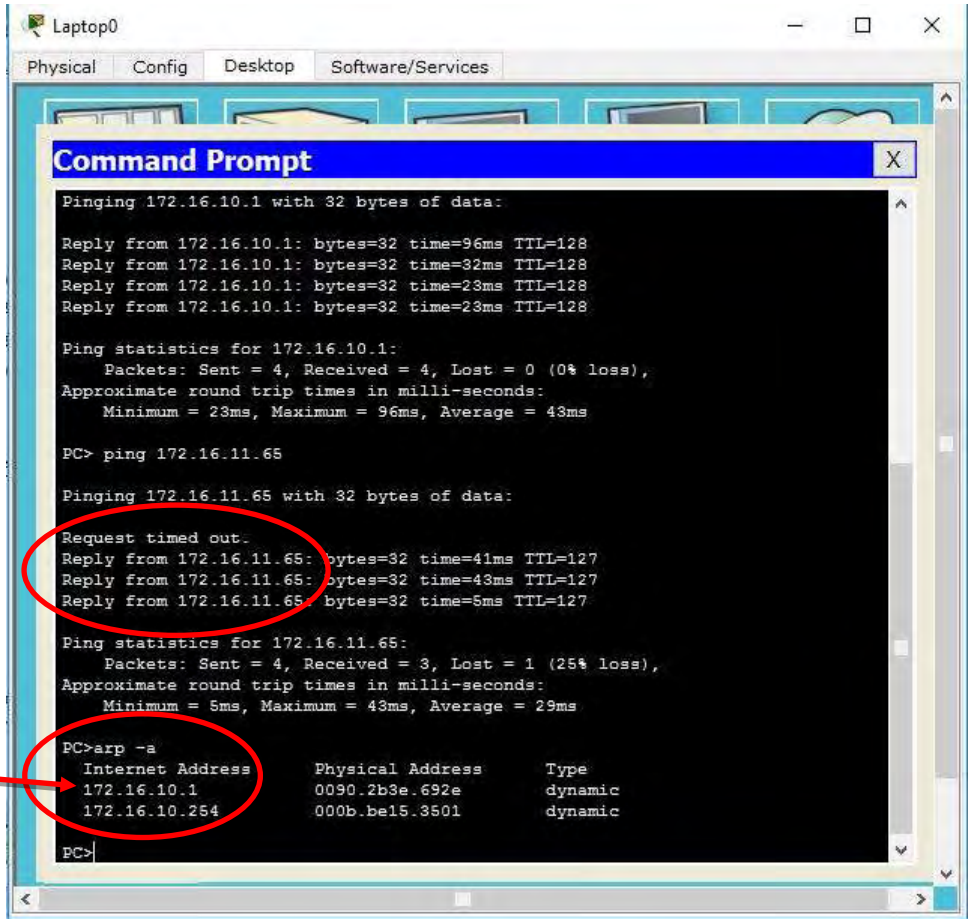
Παρακάτω, παρουσιάζονται κάποιες δοκιμές (με ping) που έγιναν στο δίκτυο προκειμένου να γίνει έλεγχος επικοινωνίας μεταξύ των άκρων:

Στην παρακάτω εικόνα φαίνεται ότι υπάρχει επικοινωνία μεταξύ του Laptop και του PC1. Να σημειωθεί ότι ο πιο απλός τρόπος να γίνει ο παραπάνω έλεγχος είναι η εντολή "ping" στο command prompt.



Εικόνα 50: Ping από το Laptop στο PC1.

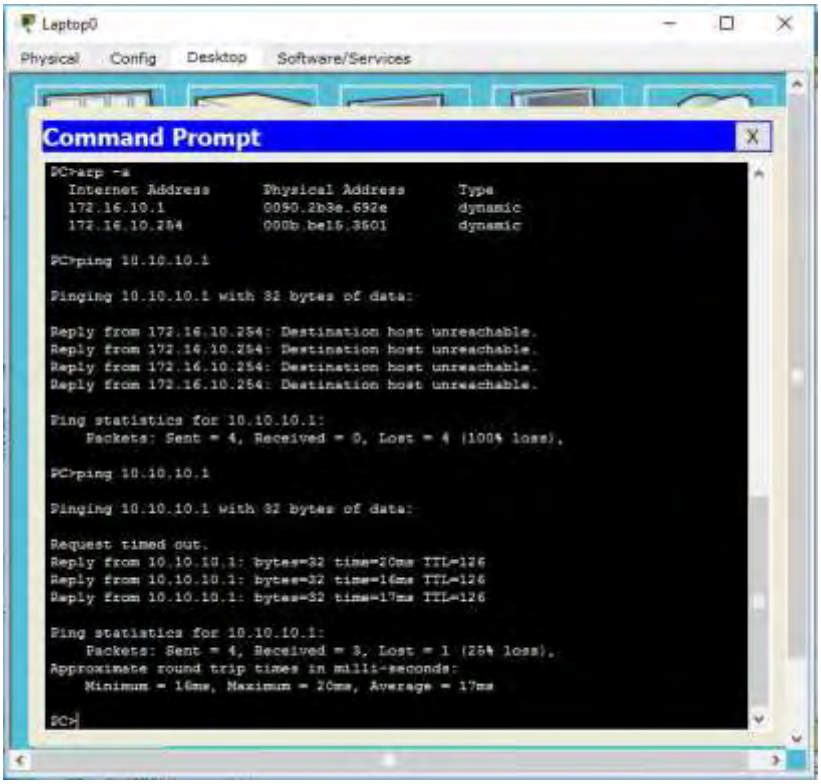
Στη συνέχεια δοκιμάζουμε από το Laptop στο PC3. Η επικοινωνία δρομολογείται μέσω του router R1 (εικόνα 50). Στην εικόνα παρατηρούμε ότι η πρώτη προσπάθεια επικοινωνίας είναι timed out, γιατί ο router απαιτεί κάποιο χρόνο να δρομολογήσει το πακέτο σε ένα άλλο VLAN από αυτό που προέρχεται. Απαιτείται λοιπόν λίγος χρόνος για να φτιαχτεί ο πίνακας arp. Αυτό το πρωτόκολλο χρησιμοποιεί τις mac address των συσκευών για να φτιάξει έναν πίνακα δρομολόγησης.



172.16.10.254
ip router R1

Εικόνα 51: Ping από το Laptop στο PC3.

Παρακάτω δοκιμάσαμε την επικοινωνία μεταξύ του Laptop και του Server 1 (Internet).



Εικόνα 52: Ping από το Laptop στο Server 1 (Internet).

Επιπρόσθετα, μπορούμε να ορίσουμε μια διεύθυνση http στο Server 1 για να βλέπουμε την ιστοσελίδα από οποιοδήποτε χρήστη του δικτύου.

Άρα, πάω στο Server 1:

Server 1 -> Services -> HTTP -> index.html -> edit ->

```
<html>
<center><font size='+2' color='blue'>Cisco Packet Tracer</font></center>
<hr>Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

ΜΕΤΑ ΤΙΣ ΑΛΛΑΓΕΣ:

```
<html>
<center><font size='+2' color='blue'>External Web Server</font></center>
<hr>Welcome to www.ext.uth.gr
<hr>Thank you for your attention!!
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

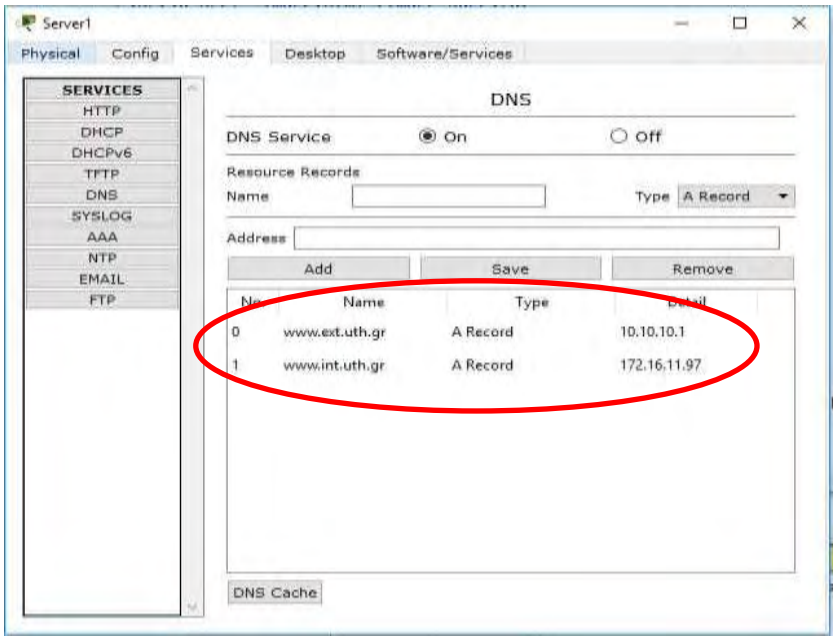
Όμοια παω και στον άλλον server και κανω το ιδιο.

```
<html>
<center><font size='+2' color='blue'>Internal Web Server</font></center>
<hr>Welcome to www.int.uth.gr
<hr>Thank you for your attention!!
<p>Quick Links:
<br><a href='helloworld.html'>A small page</a>
<br><a href='copyrights.html'>Copyrights</a>
<br><a href='image.html'>Image page</a>
<br><a href='cscoptlogo177x111.jpg'>Image</a>
</html>
```

Άρα, πάω στο **Server 1 --> Services --> DNS** και ορίζω τις παραπάνω διευθύνσεις:

Name: www.ext.uth.gr
Address: 10.10.10.1
Add
DNS Service: On

Name: www.int.uth.gr
Address: 172.16.11.97
Add
DNS Service: On



Εικόνα 53: Ορισμός http διεύθυνσης στο Server 1.

Οπότε, μπορούμε να έχουμε πρόσβαση στις ιστοσελίδες που φτιάξαμε από τους υπολογιστές του δικτύου. Παρακάτω θα δοκιμάσουμε μέσα από το laptop να μπούμε στις ιστοσελίδες που φτιάξαμε στους δύο servers. Στο packet tracer, αυτό γίνεται ως εξής:

Laptop → desktop → web browser → www.ext.uth.gr ή

Laptop → desktop → web browser → 172.16.11.97

Στον web browser του laptop, μπορούμε να πληκτρολογήσουμε είτε την ip του server είτε το όνομα της ιστοσελίδας. Στις δύο παρακάτω εικόνες, φαίνεται η πρόσβαση στις δύο αυτές ιστοσελίδες και με τους δύο προαναφερθείς τρόπους.

Εικόνα 54: Πρόσβαση στην ιστοσελίδα του Internet Server από το Laptop.

Εικόνα 55: Πρόσβαση στην ιστοσελίδα του Intranet Server από το Laptop.

Παραμετροποίηση χαρακτηριστικών ασφαλείας στο δίκτυό μας.

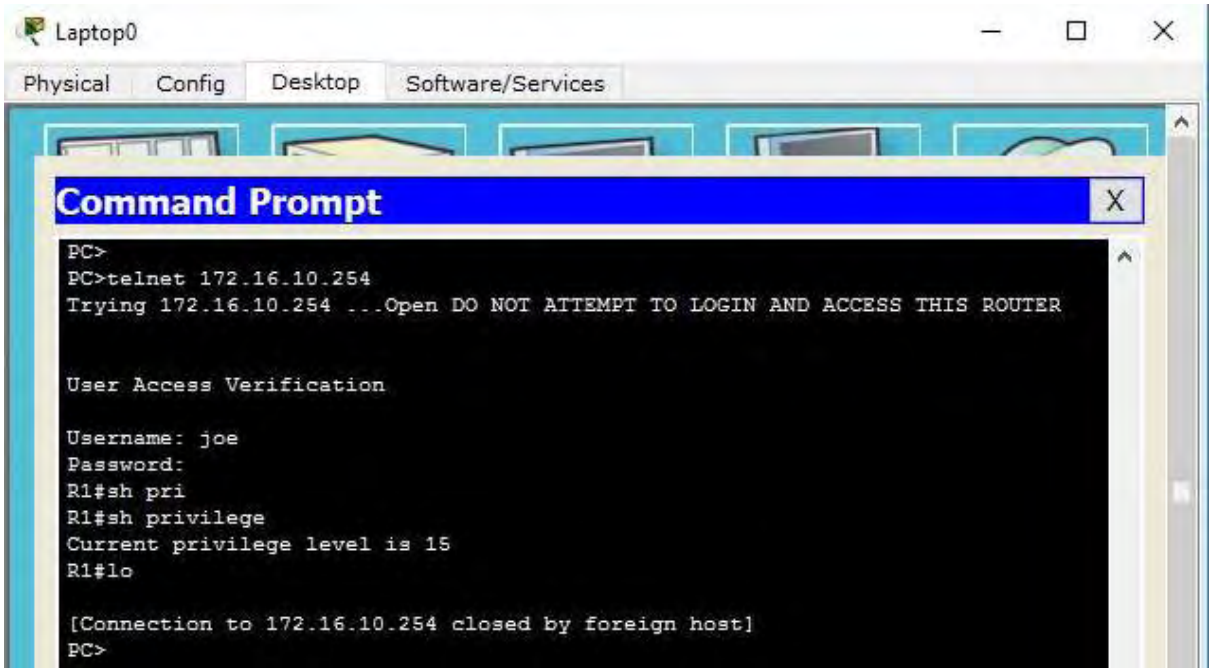
Ως τώρα εκτός από την απομακρυσμένη πρόσβαση από το Laptop δεν έχουμε πουθενά κωδικούς πρόσβασης. Άρα, το δίκτυό μας δεν είναι ασφαλές. Οπότε, παρακάτω θα δούμε μερικούς τρόπους προκειμένου να κάνουμε το δίκτυό μας λίγο πιο ασφαλές. Αρχικά, μπορούμε να βάλουμε ένα κωδικό πρόσβασης στο cisco router R1. Αυτό γίνεται ως εξής:

Συσκευή: cisco router 1 (R1)	
Εντολή	**Περιγραφή**
R1(config)#**security passwords min-length 8**	Ορίζουμε ότι ο κωδικός πρόσβασης που θα , πρέπει ο χρήστης να εισάγει για να εισέλθει στο Router, θα πρέπει να αποτελείται από 8 χαρακτήρες. Τον καθ' αυτό κωδικό θα τον ορίσουμε παρακάτω.
R1(config)#**username bob secret november**	Ορίζουμε όνομα χρήστη " bob" και κωδικό πρόσβασης "november Ο κωδικός πρόσβασης, παρατηρούμε, ότι αποτελείται από 8 χαρακτήρες. Επίσης, η λέξη "secret" σημαίνει ότι ο κωδικός που θέσαμε θα είναι κωδικοποιημένος και δεν θα φαίνεται ούτε με την εντολή "show running-config".
R1(config)#**username olga december**	Μπορούμε να ορίσουμε και ένα δεύτερο όνομα χρήστη με κωδικό που δεν είναι κρυπτογραφημένος. Άρα, έχουμε δυο ενεργούς κωδικούς για είσοδο στο Router (R1) (έναν κρυπτογραφημένο και έναν μη-κρυπτογραφημένο).
R1(config)#**line console 0**	Ρύθμιση της θύρας console του router. Οπότε θα ορίσουμε παρακάτω κωδικό πρόσβασης σε όποιον συνδέεται στο router μέσω της θύρας αυτής.

R1(config-line)# **login local**	Ορίζουμε που θα μας ζητάει τον παραπάνω κωδικό πρόσβασης.
R1(config-line)#**exec-timeout 1 30**	Ορίζουμε το χρόνο για τον οποίο αν μείνει αδρανές το router τότε θα κάνει αυτόματα logout. Ορίσαμε το χρόνο αυτό στο 1’ και 30’’.
R1(config)#**login block-for 120 attempts 5 within 45**	Η εντολή αυτή απαγορεύει την είσοδο του χρήστη για 120''=2' αν κάνει 5 αποτυχημένες προσπάθειες να μπει με το σωστό username & password στο router.
R1(config)#**banner motd # DO NOT ATTEMPT TO LOGIN AND ACCESS THIS ROUTER #**	Ορίζουμε στο cisco router να εμφανίζει ένα μήνα όταν κάποιος χρήστης προσπαθεί να εισέλθει στο router. Το μήνυμα που εμφανίζεται είναι: «Μην προσπαθείτε να εισέλθετε στο router».
R1# **log out**	Αποσύνδεση από το router. Τώρα πλέον, πρέπει ο χρήστης να εισάγει κωδικό πρόσβασης για να εισέλθει στο Router.
R1(config)#**enable password september**	Ορίζουμε να έχουμε κωδικό πρόσβασης όταν θέλουμε να εισέλθουμε στην παραμετροποίηση του router. Ο κωδικός αυτός θα είναι η λέξη “September”.
R1(config)#**enable secret ciscocisco**	Ορίζουμε να έχουμε επίσης κωδικοποιημένο (secret) κωδικό πρόσβασης όταν θέλουμε να εισέλθουμε στην παραμετροποίηση του router. Ο κωδικός αυτός θα είναι “ciscocisco”.
R1(config)#**service password-encryption**	Με την εντολή αυτή θα αποκωδικοποιήσουμε και τους κωδικούς που φαίνονται τώρα κανονικά στο “show running-config”. (september & december)
R1(config)#**username joe privilege 15 secret network4321**	Τέλος, επιλέξαμε να δημιουργήσουμε ένα χρήστη ως administrator. Το όνομα χρήστη θα είναι το “joe”, το επίπεδο δικαιοδοσίας που θα έχει ο χρήστης ορίστηκε ως το ανώτερο (privilege 15) και τέλος, επιλέγουμε ως κρυπτογραφημένο κωδικό πρόσβασης “network4321”. Παρατηρούμε ότι εδώ δεν χρειάζεται να κάνουμε enable για να μπορέσουμε να γράψουμε εντολές στο router. Να επισημάνουμε ότι στα κατώτερα privilege levels, πρέπει να ορίσουμε τι εντολές θα μπορεί να εκτελέσει κάθε χρήστης στο cisco router.

Πίνακας 10: Παραμετροποίηση του cisco router 1 - Δίκτυο 2 – μέρος 3.

Εάν στο σημείο αυτό δοκιμάσουμε από το laptop να μπούμε στη διεύθυνση 172.16.10.254 του cisco router με χρήση του πρωτοκόλλου telnet (βλ. εικονα 19), δηλαδή να συνδεθούμε σε αυτό για να υο παραμετροποιήσουμε, θα παρατηρήσουμε ότι το laptop στέλνει πακέτα (εντολές του χρήστη) στο access point, στη συνέχει στο switch και τέλος στο cisco router R1.



Εικόνα 56: Είσοδος στο cisco router με telnet από το laptop.

Όμως, χρησιμοποιούμε telnet το οποίο μεταφέρει πακέτα με χαρακτήρες ASCI, πράγμα το οποίο σημαίνει ότι μπορείς εύκολα να αναλύσει κάποιος με οποιοδήποτε protocol analyzer τα πακέτα που στέλνουμε. Άρα, δεν επιθυμούμε να χρησιμοποιήσουμε telnet για απομακρυσμένη πρόσβαση στο cisco router με telnet για λόγους ασφαλείας. Οπότε, θα ορίσουμε στο router R1 SSH access:

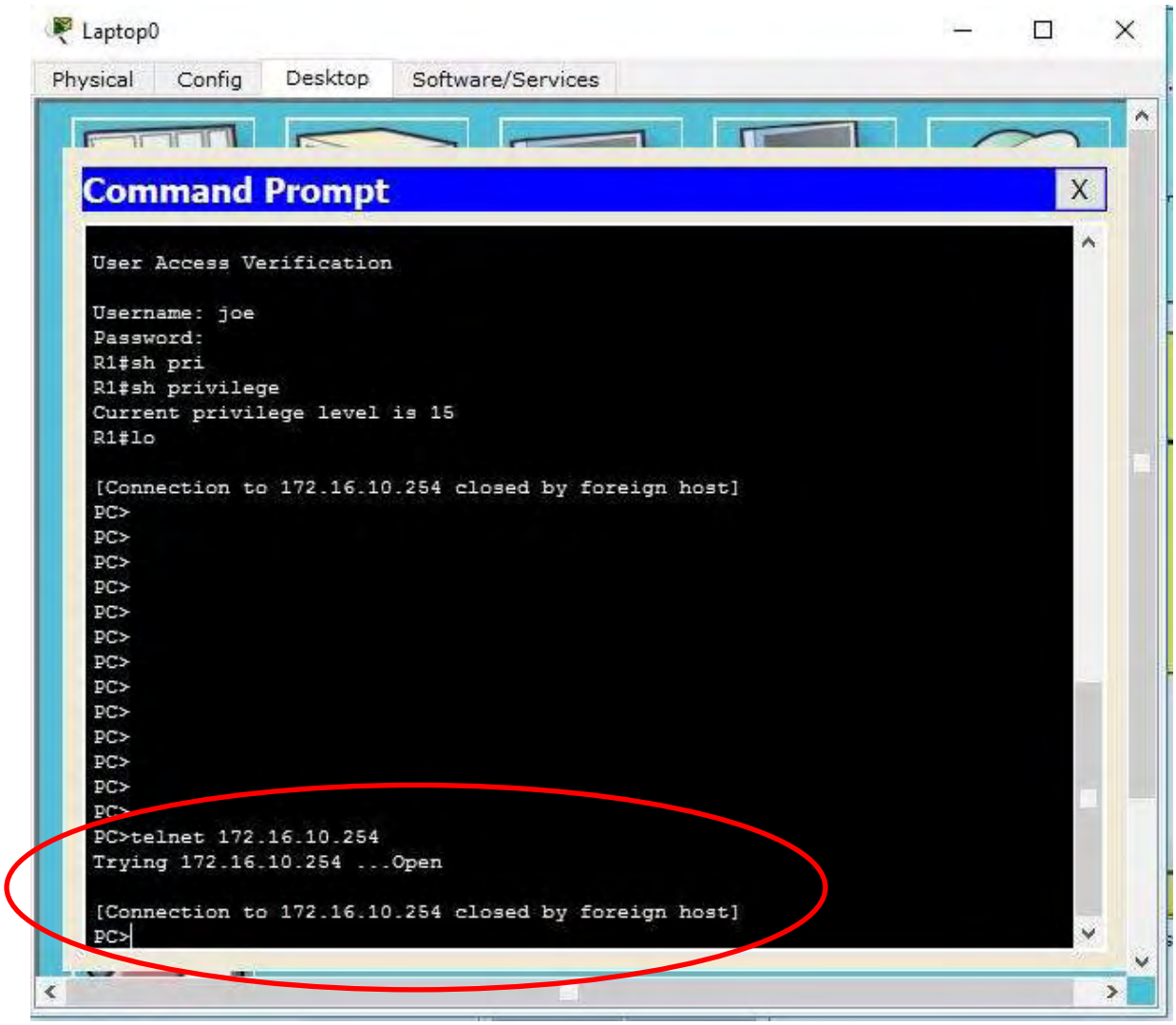
Σημείωση: Για χρήση του SSH δεν μπορούμε να χρησιμοποιήσουμε το default όνομα του router. Στην περίπτωσή μας, το έχουμε ήδη αλλάξει σε R1.

Συσκευή: cisco router 1 (R1)	
Εντολή	**Περιγραφή**
R1(config)#**ip domain-name remotetrainingsolutions**	Παραμετροποιούμε το domain name του DNS server. Επιλέξαμε “remotetrainingsolutions”.
R1(config)#**crypto key generate rsa 2048**	Μεταξύ των δύο σημείων που ανταλλάσσονται δεδομένα επιλέγουμε να αρχικοποιείται η επικοινωνία με ένα κλειδί 2048 bits.
R1(config)#**line vty 0 4**	Πρέπει να ορίσουμε το transport input να μην είναι στο default που είναι ουσιαστικά το telnet.

R1(config-line)#**transport input ssh**	Ορίζουμε το SSH.

Πίνακας 11: Παραμετροποίηση του cisco router 1 - Δίκτυο 2 – μέρος 4.

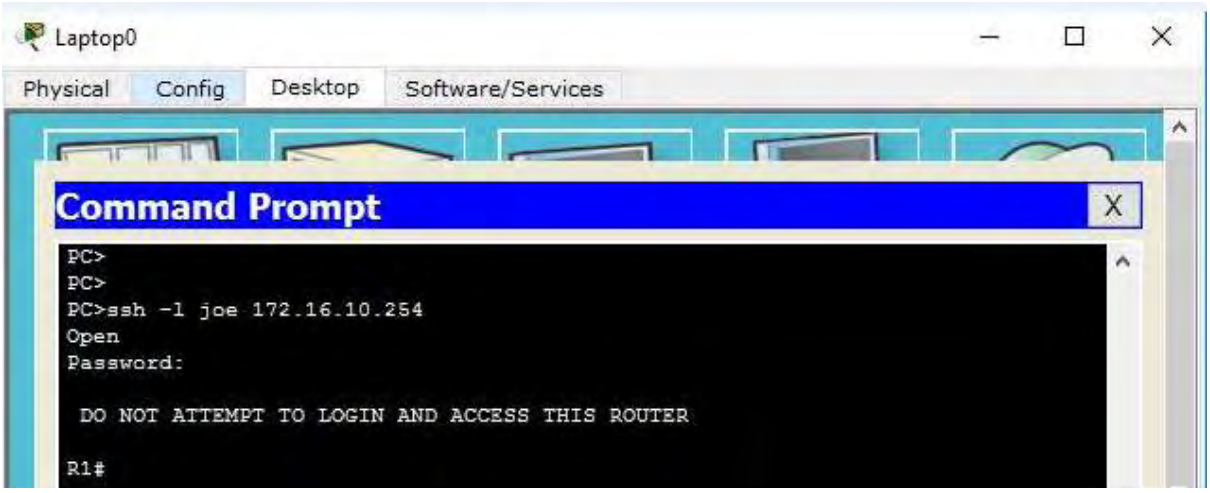
Στο σημείο αυτό θα δοκιμάσουμε να δούμε εάν λειτουργεί. Οπότε, στο laptop κάνουμε το ίδιο πείραμα με το telnet. Παρατηρούμε ότι πλέον δεν έχουμε δυνατότητα να συνδεθούμε στο router μέσω telnet.



Εικόνα 57: Telnet στο cisco - αποτυχία σύνδεσης.

Δοκιμάζουμε τώρα με ssh. Το telnet δε διαθέτει καθόλου encryption σε αντίθεση με το ssh που έχει πολύ ισχυρό encryption.

Άρα, μπορώ πλέον απομακρυσμένα (μέσω ενός laptop για παράδειγμα συνδεδεμένο στο δίκτυο) να διαχειριστώ το cisco router.



Εικόνα 58: Σύνδεση με SSH στο cisco router μέσω του laptop.

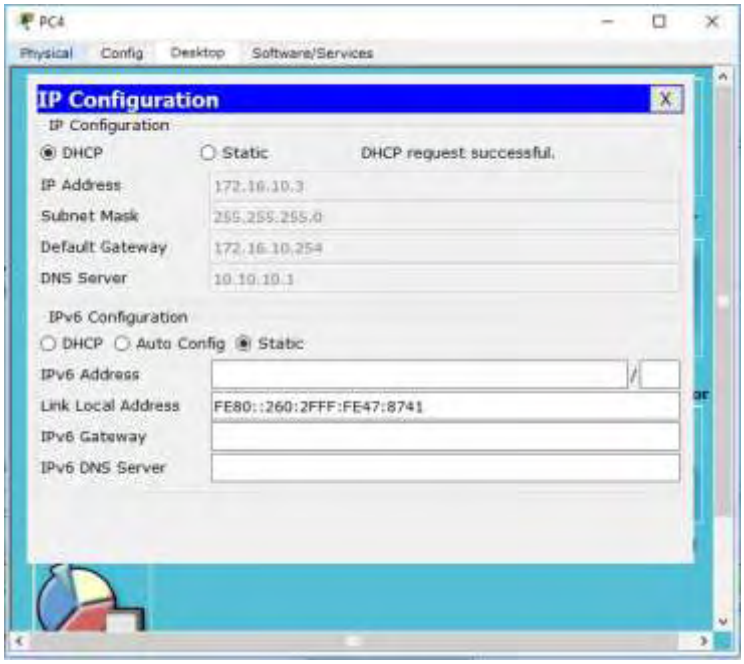
Στην παραμετροποίηση του switch 0 (SW1), μπορούμε να δούμε ότι το interface FastEthernet0/3 ανήκει στο vlan 10 με χαρακτηριστικά switchport access vlan 10 & switchport mode access. Θα ενεργοποιήσουμε την ασφάλεια port-security.

Συσκευή: switch 0 (SW1)	
Εντολή	**Περιγραφή**
SW1(config)# **interface fastEthernet 0/3**	Είσοδος στο interface fastEthernet 0/3.
SW1(config-if)#**switchport port-security mac-address sticky**	Εάν γνωρίζαμε τη mac address μπορούσαμε να τη βάλουμε κατευθείαν στην εντολή αυτή. Όμως, επειδή δεν τη γνωρίζουμε γιατί η συσκευή στο fastethernet 0/3 inteface δεν είναι συνδεδεμένη αυτή τη στιγμή, επιλέγουμε τη λέξη “sticky” που σημαίνει να κρατήσει τη mac address της πρώτης συσκευής που θα συνδεθεί σ’ αυτό το interface.
SW1(config-if)#**switchport port-security violation shutdown**	Η εντολή αυτή σημαίνει ότι εάν δεχτεί το switch πακέτα από μια συσκευή που δεν γνωρίζει τη mac-address, θα απορρίψει τα πακέτα, με αποτέλεσμα να "κλείσει" τη συγκεκριμένη πόρτα επικοινωνίας.
SW1(config-if)#**switchport port-security maximum 1**	Μέγιστος αριθμός mac-addresses που θα «κρατήσει» το switch.

Πίνακας 12: Παραμετροποίηση του switch 0 (SW1)- Δίκτυο 2 – μέρος 2.

Μπορούμε να δούμε τώρα στο configuration του switch, όλα όσα προγραμματίσαμε παραπάνω, δηλαδή: interface FastEthernet0/3 → switchport access vlan 10, switchport mode access, switchport port-security, switchport port-security mac-address sticky.

Θα δοκιμάσουμε να συνδέσουμε το pc4 στο switch (SW1). Η σύνδεση θα γίνει με straight καλώδιο. Το pc αυτό δεν έχει ακόμα ip address, καθώς δεν του έχουμε ορίσει ακόμα, αλλά έχει mac address. Θα ορίσουμε αρχικά DHCP ip address.

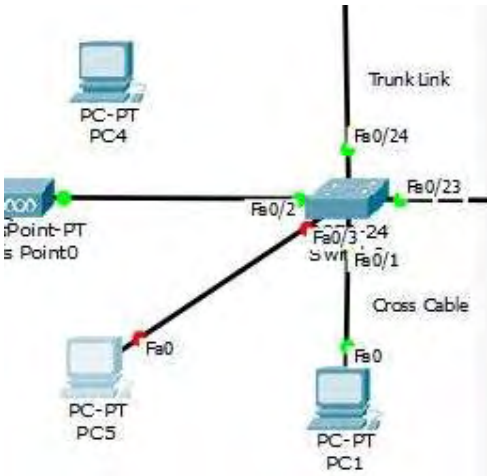


Εικόνα 59: DHCP Address pc4.

Άρα, το switch θα δεσμεύσει την mac-address αυτού του υπολογιστή (0060.2F47.8741). Για να το ελέγξουμε, θα συνδέσουμε ακόμα ένα υπολογιστή (PC5). Πιο συγκεκριμένα θα αποσυνδέσουμε το καλώδιο από αυτό τον υπολογιστή (PC4) και θα το συνδέσουμε στον άλλον υπολογιστή (PC5). Ουσιαστικά, συνδέουμε το PC5 στο switch (SW1).

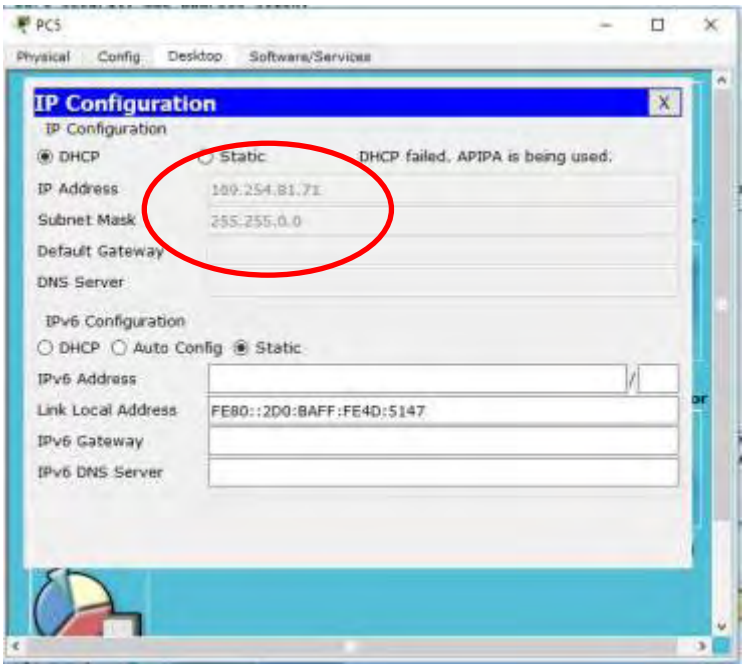
Βλέποντας το configuration του switch εκ νέου, βλέπουμε ότι το SW1 έχει αποθηκεύσει τη mac-address του PC4. Έτσι ο καινούριος υπολογιστής που συνδέθηκε δεν έχει access από το switch (switchport port-security mac-address sticky 0060.2F47.8741 // mac-address PC4).

Αν στο PC5 ορίσουμε DHCP ip address, τότε παρατηρούμε ότι οι πόρτες στα άκρα του PC5 και του SW1 switch εμφανίζουν κόκκινη βούλα, πράγμα το οποίο σημαίνει ότι δεν υπάρχει επικοινωνία.



Εικόνα 60: PC5-SW1 απώλεια επικοινωνίας.

Αυτό γίνεται για το switch καταλαβαίνει ότι αυτός ο υπολογιστής δεν έχει τη σωστή mac-address. Επίσης παρατηρούμε ότι ο υπολογιστής δεν παίρνει σωστή ip από τον dhcp server.



Εικόνα 61: Λανθασμένη IP του PC5.

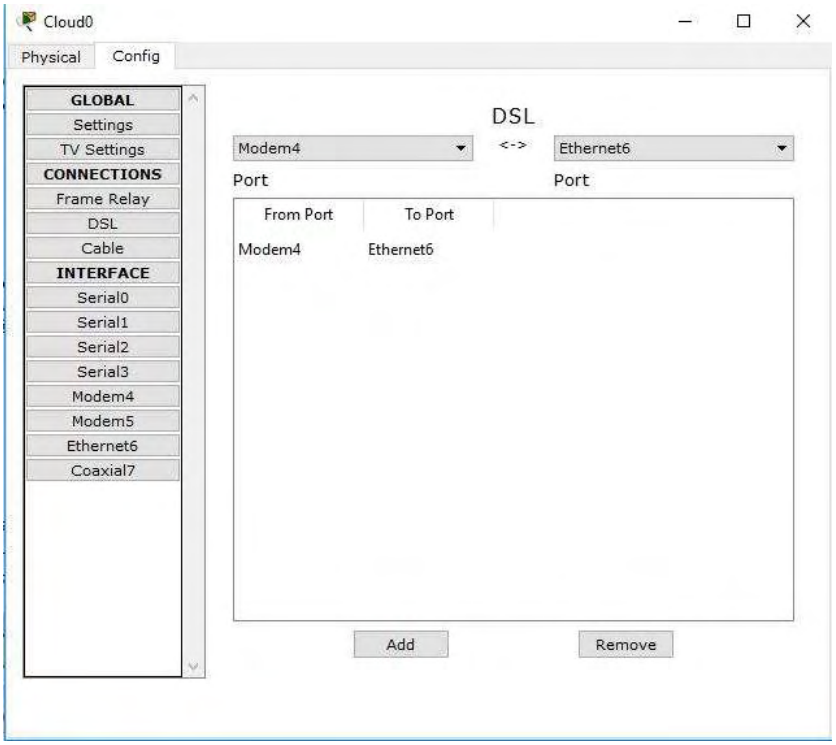
Remote Access VPN:

Στο σημείο αυτό θα αναφερθούμε στον απομακρυσμένο χρήστη που πρόκειται να συνδεθεί στο δίκτυό μας. Τα βήματα που θα ακολουθήσουμε είναι:

- Παραμετροποίηση ενός remote user – φυσική σύνδεση (modem & cloud).
- Παραμετροποίηση AAA.
- Παραμετροποίηση Remote Access VPN.
- Δοκιμές.

Επιλέγουμε στο cisco packet tracer για την προσομοίωσή μας, έναν υπολογιστή, ένα DSL Modem και ένα Cloud. Συνδέουμε τον υπολογιστή με το DSL Modem με straight καλώδιο. Τα προφίλ που επιλέγουμε είναι Fast Ethernet 0 με Port 1 αντίστοιχα και με RJ25 ακροδέκτες. Συνδέουμε το DSL Modem με το Cloud με τηλεφωνικό καλώδιο. Τα προφίλ που επιλέγουμε είναι: Port 0 και Modem 4. Συνδέουμε το Cloud με το cisco router R1 με straight καλώδιο (Ethernet 6 με FastEthernet 0/1). Πρέπει επίσης να αποφασίσουμε σχετικά με τις ips που θα δώσουμε. Οπότε, επιλέγουμε 72.44.20.0/28 ips για το Remote User και από την πλευρά του cisco router έστω ότι βάζουμε την 88.40.12.14 διεύθυνση.

Θα πρέπει να παραμετροποιήσουμε το Cloud. Στο cisco packet tracer, ανοίγουμε το cloud και πάω στο config. Στη συνέχεια, επιλέγουμε DSL και βλέπουμε τις πόρτες στις οποίες είναι συνδεδεμένο και προς τις δυο πλευρές και επιλέγουμε add.



Εικόνα 62: Cloud configuration.

Ξεκινάμε την παραμετροποίηση του cisco router R1, στο οποίο θα συνδεθεί ο απομακρυσμένος χρήστης.

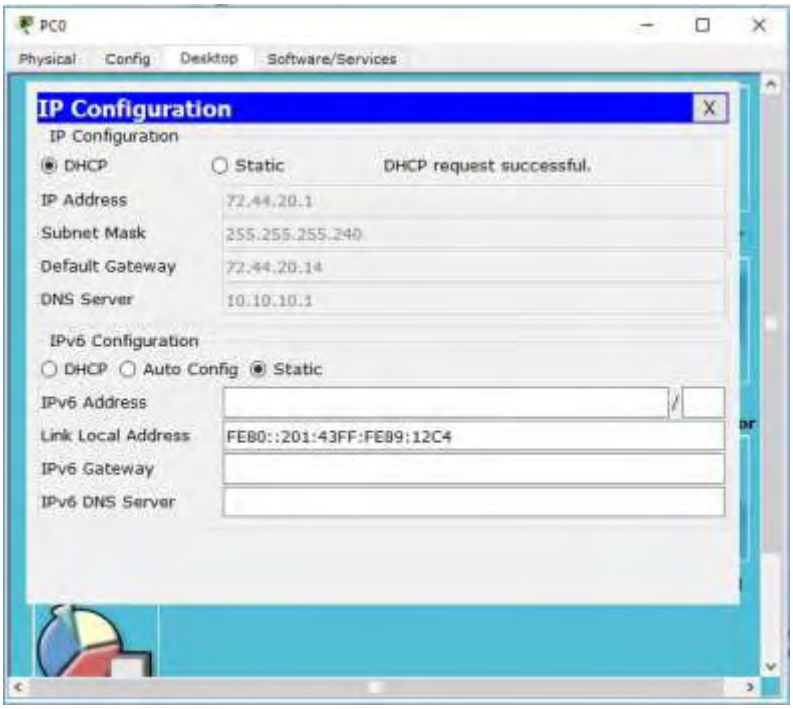
Συσκευή: cisco router 1 (R1)	
Εντολή	**Περιγραφή**
R1(config)#**interface fastEthernet 0/1**	Παραμετροποιούμε το interface στο οποίο θα συνδεθεί ο remote user.
R1(config-if)#**ip ADdress 72.44.20.14 255.255.255.240**	Ορίζουμε τη μεγαλύτερη διεύθυνση (.14) που μπορεί να πάρει ο απομακρυσμένος χρήστης, καθώς και το subnet mask (28). Το .240 προκύπτει από το 28.
R1(config-if)#**no shutdown**	Ενεργοποιούμε το interface που φτιάξαμε.
R1(config)#**ip dhcp pool REMOTE_pool**	Ορίζουμε δυναμικές ips σε όλους τους απομακρυσμένους χρήστες.
R1(dhcp-config)#**network 72.44.20.0 255.255.255.240**	Ορίζουμε τις διαθέσιμες IPs και subnet mask στους απομακρυσμένους χρήστες.
R1(dhcp-config)#**default-router 72.44.20.14**	Ορίζουμε το Default Router στους απομακρυσμένους χρήστες.

R1(dhcp-config)#**dns-server 10.10.10.1**	Ορίζουμε το Dns Server στους απομακρυσμένους χρήστες.
R1(config)#**aaa new-model**	Τα τρία aaa, χρησιμοποιείται για την ασφάλεια του δικτύου, δηλαδή απαγορεύει στους μη διαπιστευμένους χρήστες να εισέρχονται και να χρησιμοποιούν το δίκτυο.
R1(config)#**aaa authentication login REMOTE local**	Το πρώτο “a” σχετίζεται με το “authentication”. Η πιστοποίηση της ταυτότητας των χρηστών των παρεχόμενων υπηρεσιών / εφαρμογών (authentication). (REMOTE είναι το όνομα της λίστας “authentication”).
R1(config)#**aaa authorization network REMOTE local**	Το δεύτερο “a” σχετίζεται με το “authorization”. Η εφαρμογή αποτελεσματικών πολιτικών ασφάλειας για τον έλεγχο της πρόσβασης των χρηστών στις εφαρμογές και τα δεδομένα (authorization) με βάση συγκεκριμένα δικαιώματα και σε πολλαπλά επίπεδα. (REMOTE είναι το όνομα της λίστας “authorization”).
R1(config)#**username VPN secret supersecure**	Θα δημιουργήσουμε το χρήστη VPN με κρυφό κωδικό πρόσβασης supersecure.
R1(config)#**crypto isakmp policy 10**	Ορίζει το βαθμό “priority” της πολικής προστασίας που θα εφαρμοστεί <1-10000>, καθώς και της κωδικοποίησης με τα κλειδιά με τα οποία θα ανταλλάσσονται τα δεδομένα μέσα στο VPN.
R1(config-isakmp)#**encryption aes 256**	Επιλέγουμε την πιο ισχυρή και γρήγορη κωδικοποίηση (256).
R1(config-isakmp)#**hash md5**	Υπάρχουν δύο είδη αλγορίθμων ασφαλείας: md5 - Message Digest 5, sha - Secure Hash Standard.
R1(config-isakmp)#**authentication pre-share**	Ο όρος “Pre-shared” σημαίνει ότι τα μέρη που ανταλλάσσουν μεταξύ τους δεδομένα, πρέπει να συμφωνήσουν σε ένα κοινό – μυστικό κλειδί που γίνεται μέρος της πολιτικής IPSec.
R1(config-isakmp)#**group 2**	Ο Diffie-Hellman είναι αλγόριθμος ανταλλαγής Δημοσίου Κλειδιού (Public Key Algorithm) και αποτελείται από τρία group (1,2,5).
R1(config-isakmp)#**lifetime 21600**	Διάρκεια ζωής 21600 sec.

R1(config)#**crypto isakmp client configuration group REMOTE**	Ορίζει το όνομα του group ασφαλείας (REMOTE) που πρέπει να εισάγει ο χρήστης που θα συνδεθεί στο VPN.
R1(config-isakmp-group)#**key CISCO**	Στο παραπάνω group, ορίζουμε τον κωδικό (CISCO).
R1(config-isakmp-group)#**pool MYPOOL**	Ορίζουμε το όνομα του pool που θέσαμε νωρίτερα (MYPOOL).
R1(config)#**crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac**	Ως " MYSET" ορίζουμε το όνομα του "transform set" που δημιουργούμε. Ουσιαστικά το "transform set" είναι ο συνδυασμός των πρωτοκόλλων ασφαλείας που θα χρησιμοποιήσουμε. Θέτουμε ότι έχουμε ορίσει και πιο πάνω. Έτσι ορίζουμε την ασφάλεια IPSec.
R1(config)#**crypto dynamic-map DYNMAP 10**	Δημιουργία ενός δυναμικού χάρτη (dynamic-map) με το όνομα DYNMAP και σειρά εισαγωγής στο δυναμικό χάρτη 10.
R1(config-crypto-map)#**set transform-set MYSET**	Ορίζουμε το MYSET ως transform-set.
R1(config)#**crypto map CLIENT_MAP client authentication list REMOTE**	Ορίζουμε ως authentication list την REMOTE και το συσχετίζουμε με το crypto map στον Remote User.
R1(config)#**crypto map CLIENT_MAP isakmp authorization list REMOTE**	Ορίζουμε ως authorization list την abc1 και το συσχετίζουμε με το crypto map.
R1(config)#**crypto map CLIENT_MAP client configuration address respond**	Ορίζουμε στον Remote User – Client να συνδέεται – απαντάει στο δίκτυο όταν συνδέεται στο VPN χρησιμοποιώντας τις ρυθμίσεις που κάναμε μέχρι τώρα (IPSec).
R1(config)#**crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNMAP**	Ορίζουμε στο crypto map τις ρυθμίσεις που κάναμε παραπάνω.
R1(config)#**ip local pool MYPOOL 172.16.10.150 172.16.10.200**	Ορίζει το εύρος των διευθύνσεων οι οποίες είναι διαθέσιμες να ανατεθούν σε κάθε χρήστη που συνδέεται στο VPN, καθώς και το όνομα του "pool".
R1(config)#**interface fastEthernet 0/1**	Είσοδος στο interface προς το remote user.
R1(config-if)#**crypto map CLIENT_MAP**	Εφαρμογή του crypto Map που δημιουργήσαμε. (*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON)

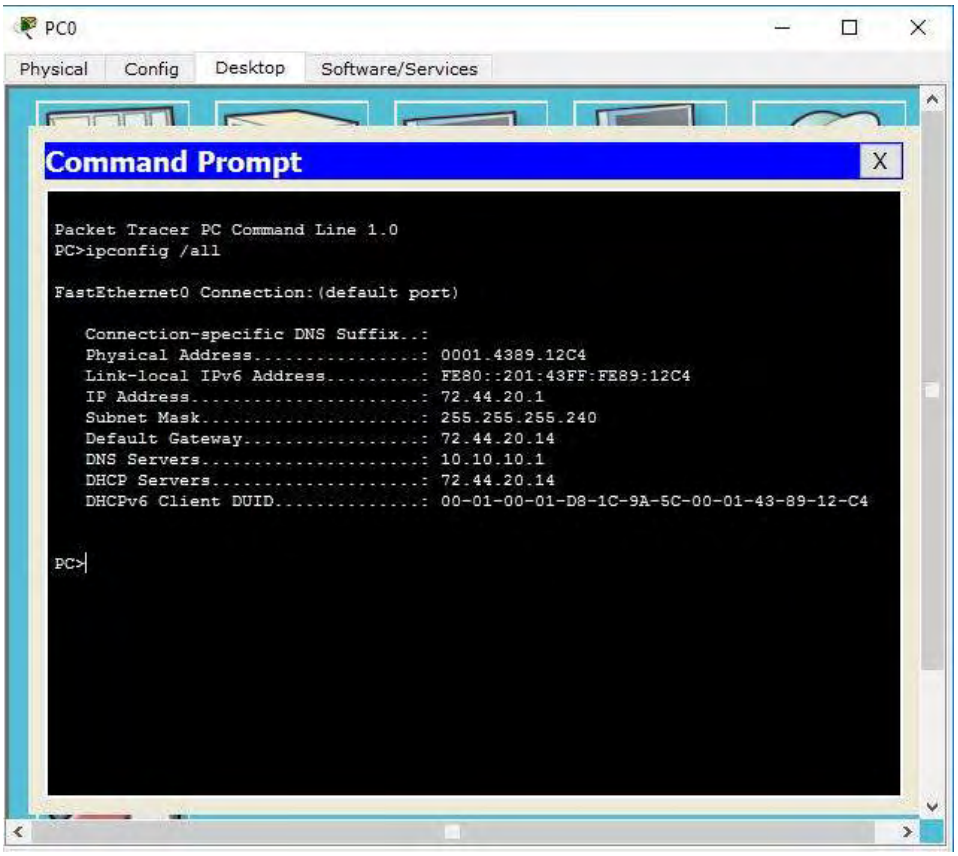
Πίνακας 13: Παραμετροποίηση του cisco router 1 - Δίκτυο 2 – μέρος 5 (VPN).

Επιλέγουμε το Remote User και ορίζουμε στον υπολογιστή να πάρει DHCP ip. (Desktop → ip Configuration) Παρατηρούμε ότι παίρνει την 72.44.20.1 με το σωστό subnet mask 255.255.255.240 και το σωστό default gateway 72.44.20.14 καθώς και dns-server 10.10.10.1.



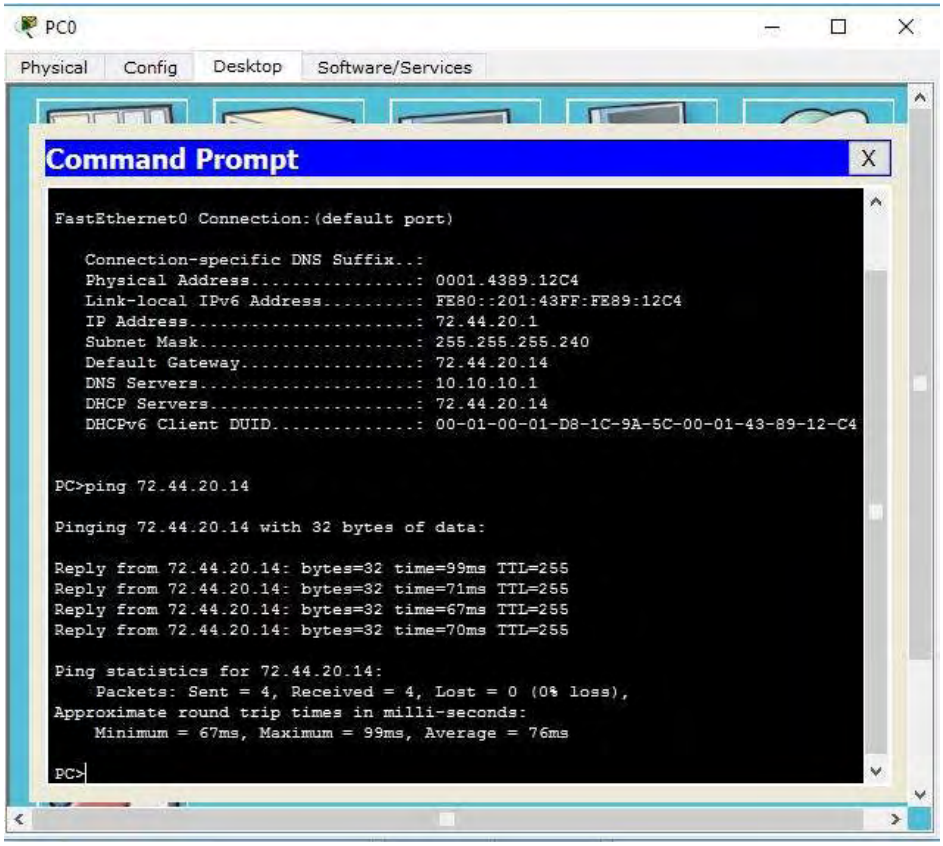
Εικόνα 63: DHCP IP Remote User Δίκτυο 2.

Επίσης, μπορώ να ελέγξω ότι ο υπολογιστής έχει πάρει σωστή ip διεύθυνση μέσω του command prompt με την εντολή ipconfig /all.



Εικόνα 64: ipconfig /all - Command Prompt Remote User Δίκτυο 2.

Δοκιμάζουμε να κάνουμε ping στο cisco router R1 και παρατηρούμε ότι απαντάει, δηλαδή έχουμε κανονικά επικοινωνία.

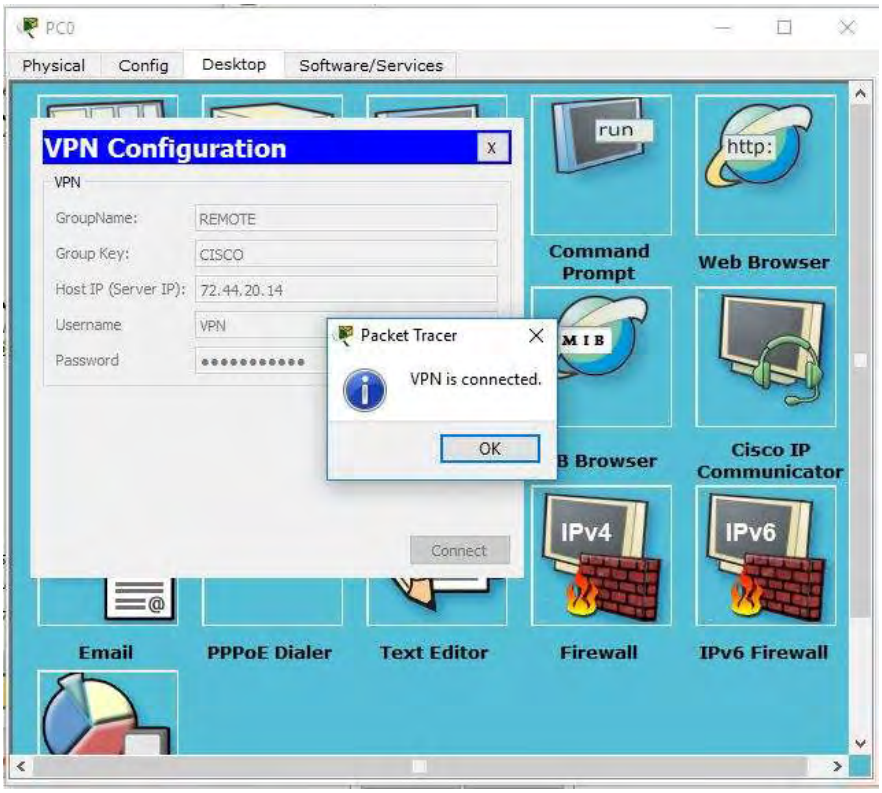


Εικόνα 65: Remote User - Router R1 - Επικοινωνία με ping – Δίκτυο 2.

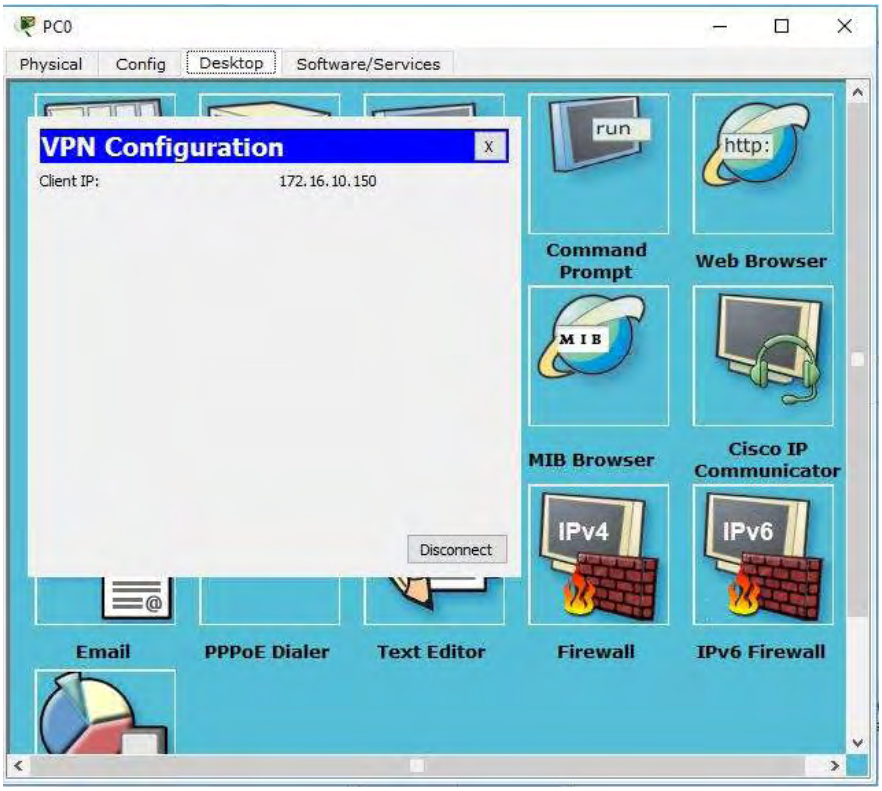
Συνδέουμε το VPN:

GroupName: REMOTE
Group Key: CISCO
Host Ip (Server IP): 72.44.20.14
Username: VPN
Password: supersecure

Βλέπουμε ότι το VPN συνδέεται κανονικά.



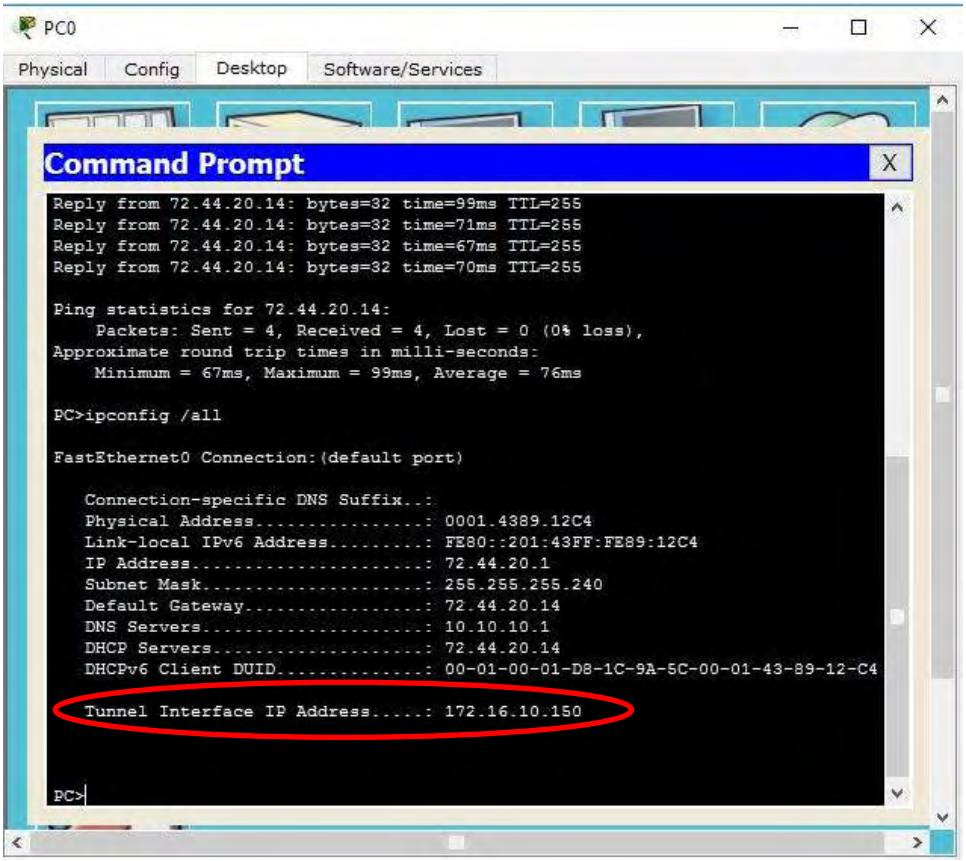
Εικόνα 66: VPN Συνδεδεμένο - Δίκτυο 2.



Εικόνα 67: Ip Remote User μετά τη σύνδεση του VPN- Δίκτυο 2.

Παρατηρούμε ότι ο υπολογιστής πήρε την πρώτη διαθέσιμη διεύθυνση από το εύρος που ορίσαμε στο ip local pool (172.16.10.150).

Εάν στο command prompt δώσουμε πάλι την εντολή ipconfig /all, θα παρατηρήσουμε ότι προστέθηκε από κάτω το "Tunnel Interface IP Address: 172.16.10.150.



Εικόνα 68: Tunnel interface ip command prompt remote user - Δίκτυο 2.

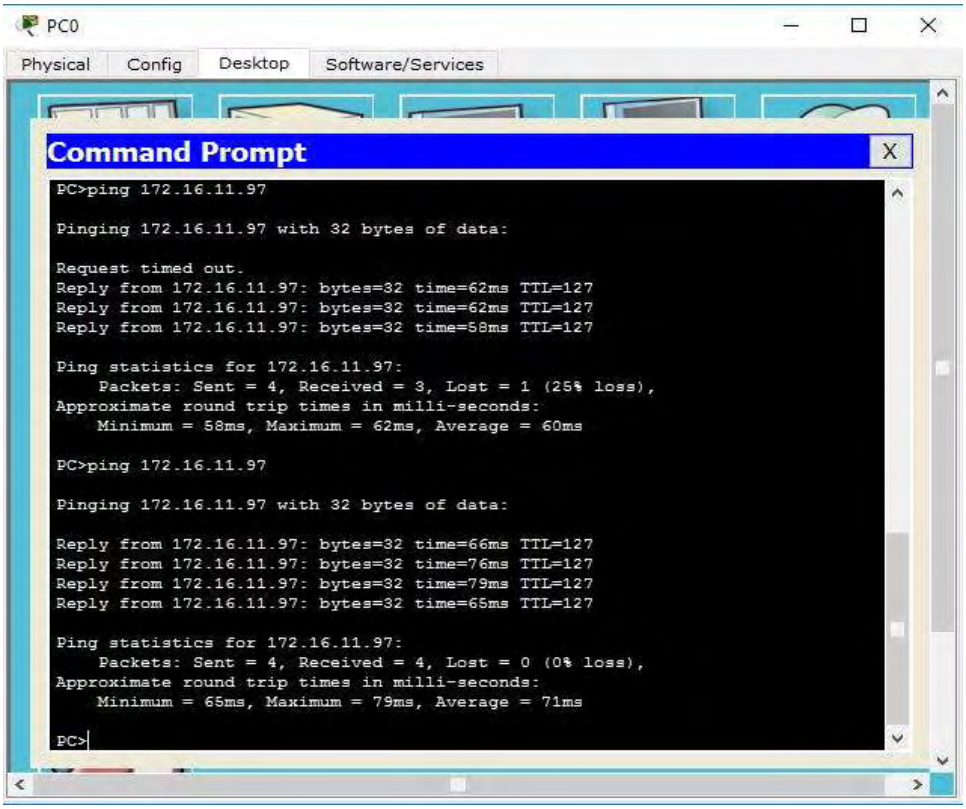
Επίσης, στο cisco router με τις εντολές **show crypto isakmp sa** και **show crypto ipsec sa** μπορούμε να διαπιστώσουμε ότι το VPN είναι συνδεδεμένο "ACTIVE".

R1#**show crypto isakmp sa**
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
72.44.20.1 72.44.20.14 QM_IDLE 1039 0 ACTIVE
IPv6 Crypto ISAKMP SA

R1#**show crypto ipsec sa**
interface: FastEthernet0/1
Crypto map tag: CLIENT_MAP, local addr 72.44.20.14 //local addr στο router
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.10.150/255.255.255.255/0/0)
current_peer 72.44.20.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 //βλέπω ότι έχω 0 πακέτα κωδικοποιημένα
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 //και 0 αποκωδικοποιημένα
#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

Εάν κάνουμε ping από το Remote User στο Server Intranet - VLAN 40, θα δούμε μέσα από την παραπάνω εντολή ότι έχουμε πλέον κάποια κωδικοποιημένα και αποκωδικοποιημένα πακέτα.



Εικόνα 69: Ping από το Remote User στο Server Intranet μέσω VPN - VLAN 40 - Δίκτυο 2.

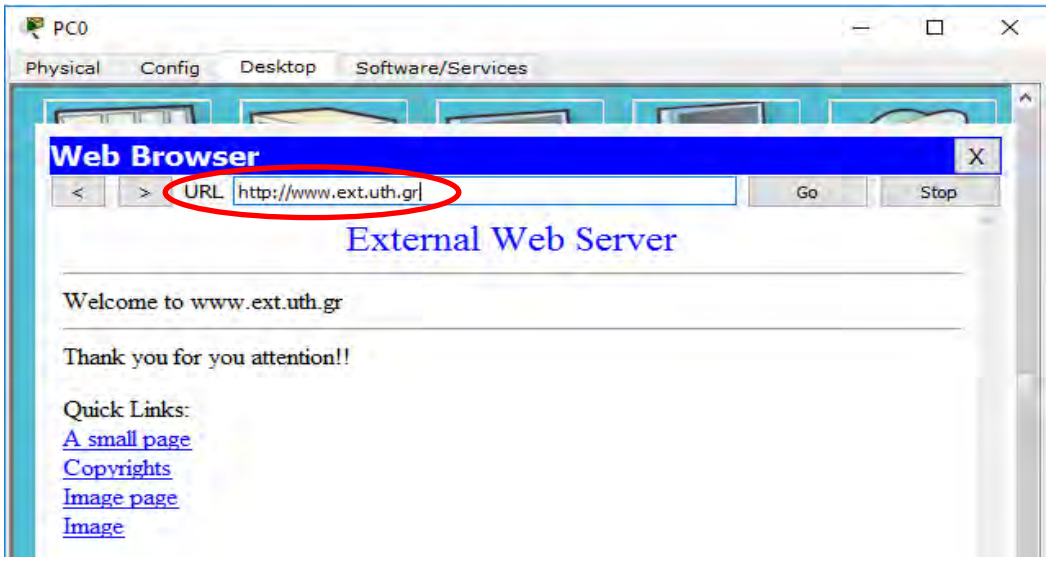
Όπως έχουμε αναφέρει και παραπάνω, το πρώτο πακέτο χάθηκε και είχαμε "timeout", καθώς ήταν η πρώτη φορά που επιχειρήσαμε επικοινωνία και έπρεπε να αρχικοποιηθεί το route. Άρα, μέσω του VPN, ο απομακρυσμένος χρήστης έχει πρόσβαση στο δίκτυο της εταιρίας. Εάν κάνουμε την ίδια δοκιμή με παραπάνω χωρίς ο απομακρυσμένος χρήστης να είναι συνδεδεμένος στο VPN, θα διαπιστώσουμε ότι δεν θα υπάρχει επικοινωνία.

R1#**show crypto ipsec sa**
interface: FastEthernet0/1
Crypto map tag: CLIENT_MAP, local addr 72.44.20.14
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.10.150/255.255.255.255/0/0)
current_peer 72.44.20.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0 //βλέπω τώρα ότι έχω 7 κωδικοποιημένα πακέτα
#pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 0 //και 8 αποκωδικοποιημενα

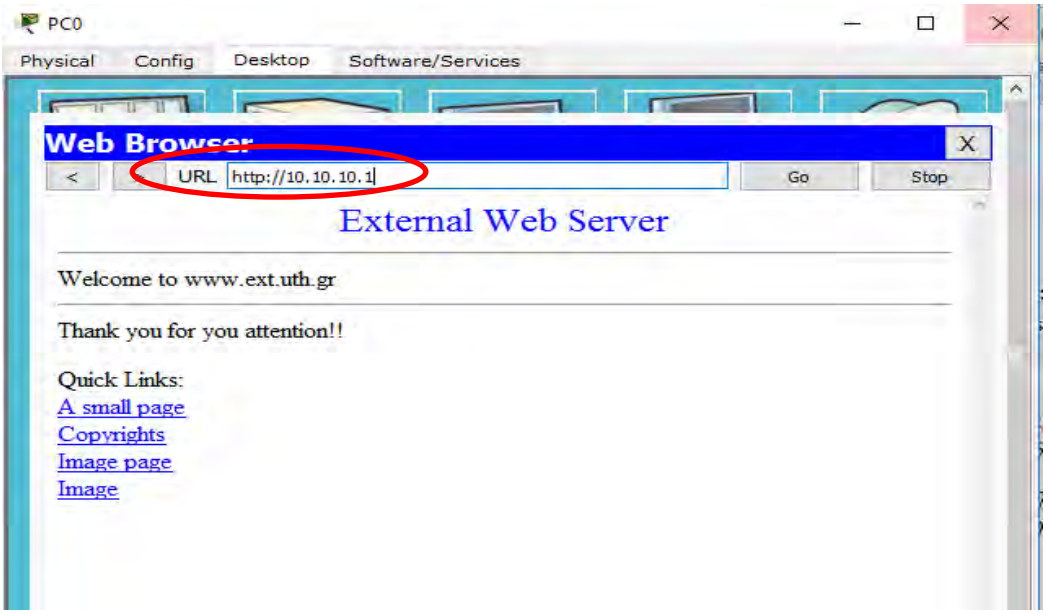
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

Στη συνέχεια, θα δοκιμάσουμε από το Remote User μέσω του Web Browser να δούμε την ιστοσελίδα που έχουμε φτιάξει στον Internet Server:

Άρα, από το web browser του laptop πληκτρολογούμε είτε τη διεύθυνση www.ext.uth.gr είτε την ip του server (10.10.10.1). Παρατηρούμε ότι βλέπουμε κανονικά τη διεύθυνση αυτή και συνεπώς έχουμε πρόσβαση στο server μέσω του VPN.

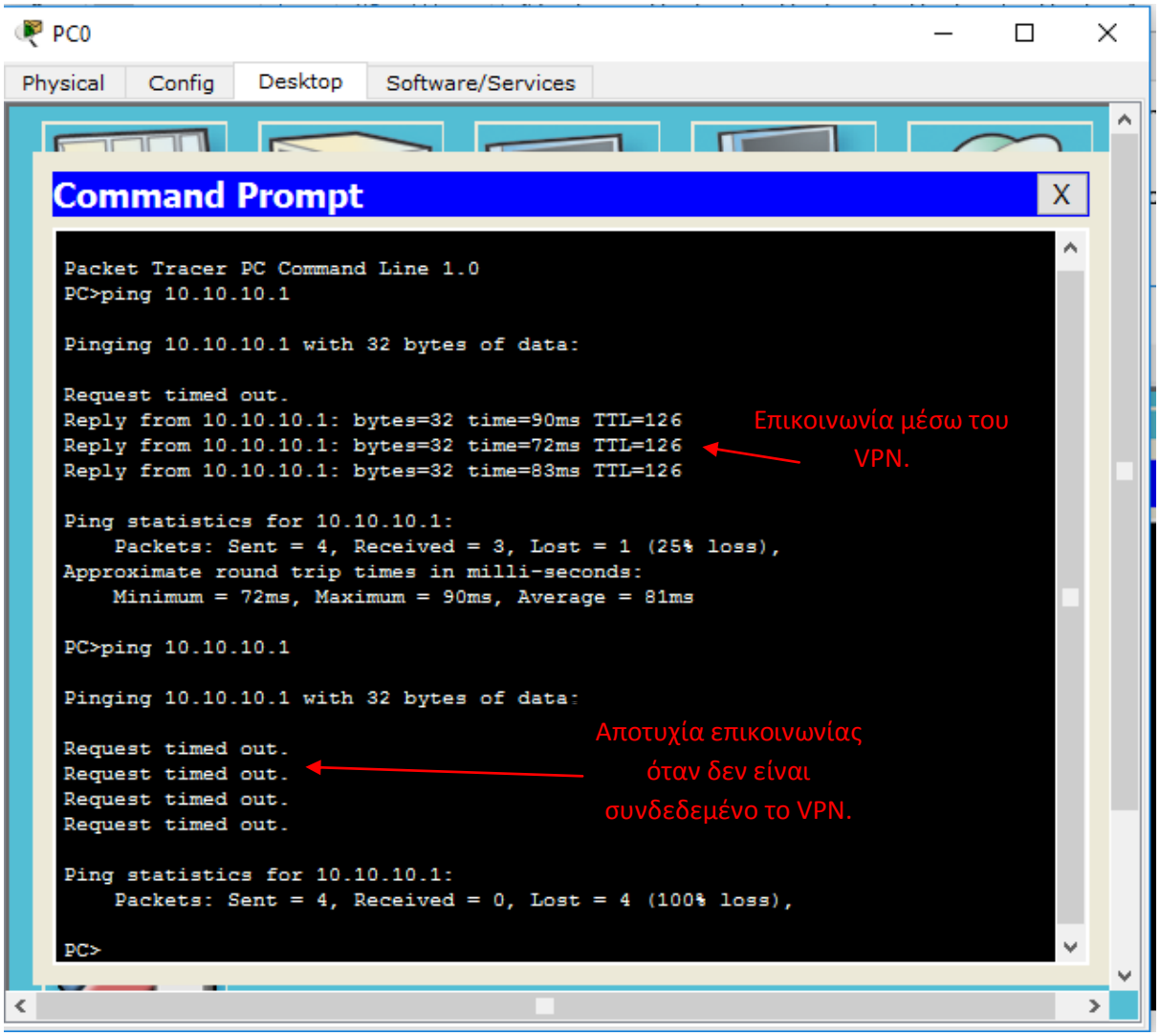


Εικόνα 70: Πρόσβαση στον Internet Server μέσω του web browser του απομακρυσμένου χρήστη (https url).



Εικόνα 71: Πρόσβαση στον Internet Server μέσω του web browser του απομακρυσμένου χρήστη (ip).

Τέλος, δοκιμάζω την επικοινωνία με τον internet server με ping από το command prompt του laptop. Βλέπουμε ότι έχουμε κανονικά επικοινωνία. Κάνουμε disconnect το VPN από τον υπολογιστή του Remote User και δοκιμάζουμε ξανά. Στην περίπτωση αυτή δεν υπάρχει επικοινωνία. Άρα το VPN λειτουργεί κανονικά.



Εικόνα 72: Ping από το laptop στον Internet Server με και χωρίς το VPN.

ΚΕΦΑΛΑΙΟ 6: ΣΥΜΠΕΡΑΣΜΑΤΑ – ΕΠΙΛΟΓΟΣ

Η τεχνολογία στον χώρο των επικοινωνιών προχωράει αλματωδώς και κάθε νέα εφαρμογή, κάθε νέα εφεύρεση, κάθε νέο project αποτελούν ισχυρά μέσα για την εκπλήρωση του σκοπού αυτού. Η μελέτη και εφαρμογή των δικτύων VPNs αντιπροσωπεύουν ένα ακόμη δείγμα της ακάθεκτης και συνεχώς επιταχυνόμενης προόδου στον τομέα αυτό.

Ένα VPN (Virtual Private Network) μπορεί να προσφέρει ευέλικτες λύσεις σε θέματα επικοινωνίας, οργάνωσης, διαχείρισης και κατανομής πληροφοριών σε όλα τα τμήματα ή τα υποκαταστήματα μιας επιχείρησης, ανεξαρτήτως γεωγραφικής απόστασης και με συγκεκριμένες εγγυήσεις, ως προς την απόδοση.

Τα βασικά πλεονεκτήματα των VPNs είναι η εξοικονόμηση κόστους, η ευελιξία που παρέχουν, καθώς προσαρμόζονται εύκολα στις ανάγκες επιχειρήσεων διαφορετικών μεγεθών και απαιτήσεων, και η ασφάλεια. Πολλές φορές σε ένα VPN η ασφάλεια έρχεται αντιμέτωπη με τη λειτουργικότητα, καθώς βασικός περιορισμός στην χρήση ισχυρών αλγορίθμων με μεγάλο μήκος κλειδιού είναι η απόδοση.

Τα IP VPNs και πιο συγκεκριμένα το πρωτόκολλο IPSec, σύμφωνα με το οποίο έγιναν και οι προσομοιώσεις στην εργασία, είναι αυτό που έχει κυριαρχήσει σε παγκόσμια κλίμακα, λόγω του χαμηλού κόστους υλοποίησης και της μεγάλης προσαρμοστικότητάς του, τόσο σε μηχανισμούς ασφαλείας, όσο και στα πρωτόκολλα διαφόρων επιπέδων με τα οποία μπορεί να συνεργαστεί, σχηματίζοντας ένα συμπαγές σύστημα. Σημειωτέον ότι το IPSec δεν απαιτεί αλλαγές στην υπάρχουσα υποδομή του δικτύου.

Αναλύθηκε ότι σε κάθε υλοποίηση VPN θα πρέπει να ληφθούν υπόψη κάποια ειδικά θέματα που αφορούν τα συστατικά του δικτύου που εφαρμόζεται, έτσι ώστε να αποφευχθούν κάποια ιδιαίτερα προβλήματα. Επιπλέον, η επιλογή του κατάλληλου τύπου VPN, των αντίστοιχων τεχνολογιών (Hardware/Software), των πρωτοκόλλων και μηχανισμών ασφαλείας, απαιτεί την λεπτομερή γνώση όλων αυτών, καθώς και των απαιτήσεων της εφαρμογής.

Για τους παραπάνω λόγους πριν την εφαρμογή ενός VPN, πρέπει να εξεταστούν αναλυτικά και με προσοχή όλες οι υπάρχουσες ρυθμίσεις και η λειτουργία του πραγματικού δικτύου, έτσι ώστε να αποφευχθούν ιδιαίτερα προβλήματα.

Επίσης, θα πρέπει η προτεινόμενη λύση να προσομοιώνεται, έτσι ώστε να αντιμετωπίζονται τυχόν προβλήματα που προκύπτουν. Με βάση την εφαρμογή στα πλαίσια της εργασία σαν καλή πρακτική είναι προτιμότερο να διαχωρίζεται η προτεινόμενη λύση σε στάδια εφαρμογής, καθώς έτσι είναι πιο εύκολη η απομόνωση και ο εντοπισμός ενός προβλήματος που μπορεί να εμφανιστεί σε μια εφαρμογή.

Επομένως, είναι αναμφισβήτητα πολύ σημαντικό να μας παρέχεται η δυνατότητα να μπορούμε να ελέγξουμε ένα δίκτυο πριν την υλοποίησή του, σε ένα εικονικό περιβάλλον.

Όπως ήδη περιγράφηκε εκτενώς, στη διπλωματική εργασία χρησιμοποιήσαμε ως λογισμικό προσομοίωσης το Cisco Packet Tracer, προκειμένου να παραμετροποιήσουμε εικονικά τις συσκευές του δικτύου μας και να μελετήσουμε τη λειτουργία του.

Το λογισμικό αυτό μπορεί να λειτουργεί σε διαφορετικές πλατφόρμες –στην εργασία αυτή χρησιμοποιήθηκε η αγγλική cross platform- το δε γραφικό περιβάλλον του, δίνει τη δυνατότητα να προσθέσουμε και να αφαιρέσουμε συσκευές δικτύου κατά βούληση. Στη διπλωματική μας, παραμετροποιήθηκαν και χρησιμοποιήθηκαν συνολική οκτώ διαφορετικές συσκευές δικτύου, οι οποίες εντάχθηκαν στις δυο τοπολογίες δικτύων που επιλέχθηκαν και υλοποιήθηκαν.

Μετά την εγκατάσταση και τη ρύθμιση των συσκευών, έγιναν οι δοκιμές τόσο σε πραγματικό χρόνο (real time), όσο και σε περιβάλλον προσομοίωσης (simulation), με τα μέρη του δικτύου να ανταλλάσσουν πακέτα δεδομένων, στα πλαίσια των λειτουργιών που ανατέθηκαν. Οι έλεγχοι του δικτύου τόσο σε πραγματικό χρόνο, όσο και στο περιβάλλον προσομοίωσης είναι πανομοιότυποι και είναι στην ευχέρεια του χρήστη επιλέξει τον τρόπο με τον οποίο θα εξετάσει το δίκτυο που έχει υλοποιήσει. Στις προσομοιώσεις μας παρουσιάσαμε και τους δύο παραπάνω τρόπους για λόγους παρουσίασης των δυνατοτήτων του εργαλείου προσομοίωσης που χρησιμοποιήσαμε, καθώς και για λόγους ποικιλομορφίας στην παρουσίαση των αποτελεσμάτων. Το Cisco Packet Tracer μας έδωσε τη δυνατότητα να παρακολουθήσουμε και να εξετάσουμε τη δρομολόγηση και τη δομή των πακέτων σε κάθε λεπτομέρεια, και να αντιμετωπίσουμε τυχόν προβλήματα που προέκυπταν.

Συμπερασματικά, το Cisco Packet Tracer είναι ένα ισχυρό πρόγραμμα προσομοίωσης δικτύου, ένα σημαντικό συμπληρωματικό βοήθημα, που επιτρέπει στους χρήστες:

- να δημιουργήσουν ένα δίκτυο με σχεδόν απεριόριστο αριθμό συσκευών,
- να πειραματιστούν με τη συμπεριφορά του δικτύου,
- να εκτελέσουν προμελετημένα σενάρια σε πραγματικό χρόνο (real time), αλλά και με ελεγχόμενο τρόπο (simulation mode),
- να πραγματοποιήσουν παρατηρήσεις στα γεγονότα που συμβαίνουν στο δίκτυο, με δυνατότητα χρήσης φίλτρων για παρατηρήσεις εξειδικευμένων συμβάντων,
- να εντοπίσουν τυχόν σφάλματα στο δίκτυο που έχουν δημιουργήσει στο περιβάλλον του Cisco Packet Tracer, να τα ελέγξουν εξονυχιστικά και να τα αντιμετωπίσουν πριν την υλοποίηση του πραγματικού δικτύου, στο οποίο ο εντοπισμός σφαλμάτων θα αποτελούσε μια χρονοβόρα διαδικασία.

Γενικότερα, το λογισμικό αυτό δίνει τη δυνατότητα εξοικειωσης με τα δίκτυα υπολογιστών. Πιο συγκεκριμένα με τη δημιουργία ενός δικτύου VPN και, χρησιμοποιώντας τον εξοπλισμό της Cisco, μελετήθηκε λεπτομερώς η δικτυακή λειτουργία. Για το λόγο αυτό χρησιμοποιώντας το λογισμικό αυτό δημιουργήσαμε αρχικά ένα μικρό δίκτυο ($1^η$ προσομοίωση) για να εστιάσουμε και να κατανοήσουμε τη λειτουργία ενός VPN και στη συνέχεια να χτίσουμε σταδιακά ένα μεγάλο δίκτυο μιας εταιρίας με επιμέρους υπο-δίκτυα VLANs ($2^η$ προσομοίωση), να τα παραμετροποιήσουμε ώστε να λειτουργούν σωστά και να συνδέσουμε στο δίκτυο της εταιρίας, μέσω ενός VPN, έναν απομακρυσμένο χρήστη. Ελέγχθηκε εξονυχιστικά η ορθή λειτουργία του δικτύου, εξασφαλίζοντας ότι ο απομακρυσμένος χρήστης συνδέεται στο δίκτυο της εταιρίας μόνο μέσω του VPN που δημιουργήσαμε. Αποδείχτηκε ότι το λογισμικό αυτό είναι εύκολο στη χρήση και εξυπηρετεί το σκοπό του φτάνει ο χρήστης να είναι εξοικειωμένος με τις διαδικτυακές τεχνολογίες επικοινωνίας.

Κλείνοντας, θα θέλαμε να τονίσουμε ότι τα VPNs αποτελούν ίσως το παρόν και το μέλλον των ιδιωτικών δικτύων, αφού η εφαρμογή τους ερευνάται και εξελίσσεται σε παγκόσμια κλίμακα, κερδίζοντας συνεχώς έδαφος στο χώρο των δικτύων. Από τη μεριά τους οι πάροχοι πρόσβασης

φροντίζουν επισταμένα για την υποστήριξη, την επέκταση και τη συνεχή διαθεσιμότητα της VPN υπηρεσίας σε κάθε περιοχή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Paul Ferguson, «What Is a VPN? - Part I,» Cisco Systems and Geoff Huston,Telstra, 2016. [Ηλεκτρονικό].

[2] «Comparison of Dial-up and Leased-Line Links,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[3] Λιμνιώτης Κώστας, Σχεδίαση Εικονικών Δικτύων, Τεχνολογικό Εκπαιδευτικό Ίδρυμα: Σημειώσεις Τμήματος Πληροφορικής και Τεχνολογίας Υπολογιστών, 2005.

[4] CISCO, «Asymmetric Digital Subscriber Line (ADSL),» [Ηλεκτρονικό]. Available: http://www.cisco.com/c/en/us/tech/long-reach-ethernet-lre-digital-subscriber-line-xdsl/asymmetric-digital-subscriber-line-adsl/index.html. [Πρόσβαση March 2017].

[5] Deuce Themes, «WHAT'S THE DIFFERENCE BETWEEN ADSL, VDSL AND FIBRE INTERNET?,» [Ηλεκτρονικό]. Available: http://deucethemes.com/whats-the-difference-between-adsl-vdsl-and-fibre-internet/. [Πρόσβαση March 2017].

[6] IN.GR, «Τι είναι το VDSL;,» December 2011. [Ηλεκτρονικό]. Available: http://tech.in.gr/short-news/?aid=1231140162. [Πρόσβαση March 2017].

[7] Capacity Media, «What is vectoring technology?,» March 2012. [Ηλεκτρονικό]. Available: http://www.capacitymedia.com/Article/2986517/What-is-vectoring-technology.html. [Πρόσβαση March 2017].

[8] whatsag.com, «2G, 3G, 4G, 4G LTE, 5G – What are They?,» [Ηλεκτρονικό]. Available: https://www.whatsag.com/. [Πρόσβαση March 2017].

[9] Dave Kosiur, Building and Managing Virtual Private Networks, : john Wiley, 1998.

[10] Εμμανουήλ Κουσλόγλου, «Το μοντέλο αναφοράς OSI ως προτυπο δτην εκπαιδευτικη διαδικασία,» 1ο Πανελληνίο Εκπαιδευτικό Συνέδριο Ημαθίας. [Ηλεκτρονικό].

[11] Σ. Μαργαρίτη, Ελ. Στεργίου, Τοπικά και Αστικά Δίκτυα LAN – MAN, ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ.

[12] «List of network protocols (OSI model),» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/List_of_network_protocols_(OSI_model).

[13] «OSI Layer To Protocol Match,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[14] Andrew S. Tanenbaum, Computer Networks, Pearson Education 4th edition, 2003.

[15] «How VPN Works,» 2003. [Ηλεκτρονικό]. [Πρόσβαση 2016].

[16] «TCP/IP Protocol,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[17] Network Protocol Handbook, Javvin Technologies Inc, 2005.

[18] Μ. Λογοθέτης, Δίκτυα επικοινωνίας Υπολογιστών, Πολυτεχνική Σχολή Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών.

[19] Himanshu Arora, «IP Protocol Header Fundamentals Explained with Diagrams,» 2012. [Ηλεκτρονικό].

[20] Silvia Hagen, IPv6 Essentials, USA: O'Reilly Media, 2014.

[21] Μαυρουδή Μαγδαληνή, «IPV6, MBONE, MOBILE IPV6, ICMPV6, IGMPV6,IPV6 OVER ATM,» [Ηλεκτρονικό].

[22] «IPV6 vs IPV4,» [Ηλεκτρονικό].

[23] Χρήστος Μπούρας, «Πανεπιστήμιο Πατρών - Δίκτυα Υψηλών Ταχυτήτων,» Ιούνιος 2005. [Ηλεκτρονικό]. [Πρόσβαση Απρίλιος 2017].

[24] Douglas Crawford, «Best VPN,» [Ηλεκτρονικό]. Available: https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/. [Πρόσβαση February 2017].

[25] Νταφούλης Σωτήριος, «Οι αρχιτεκτονικές των εικονικών ιδιωτικών δικτύων (VPN),» ΠΜΣ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ, 2005. [Ηλεκτρονικό].

[26] Matthew Castelli, Network Consultants Handbook, Cisco Press, 2002.

[27] Μοραντής Σταύρος Πανεπιστήμιο Πειραιά, «Μελέτη της τεχνολογίας MPLS (Multi Protocol Label Switching) με βάση τις προηγμένες δικτυακές υπηρεσίες,» [Ηλεκτρονικό]. Available: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/6580/MPPL09047.pdf?sequence=1. [Πρόσβαση 2017].

[28] ISLab (Internet Systematics Lab), «Secure Socket Layer (SSL),» [Ηλεκτρονικό]. Available: http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ssl.htm. [Πρόσβαση 2017].

[29] http://bigdata-madesimple.com, «VPN use and data privacy stats for 2016,» [Ηλεκτρονικό]. Available: http://bigdata-madesimple.com/vpn-use-and-data-privacy-stats-for-2016/. [Πρόσβαση March 2017].

[30] T. G. o. t. H. Kong, «VPN SECURITY,» The Government of the Hong Kong Special Administrative Region, Hong Kong, February 2008.

[31] WHITFIELD DIFFIE AND MARTIN E. HELLMAN, «New Directions in Cryptography,» *IEEE TRANSACTIONS ON INFORMATION THEORY, ,* τόμ. 22, αρ. 6, pp. 644-654, 1976.

[32] Wikipedia, «Wikipedia,» January 2017. [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Block_cipher. [Πρόσβαση February 2017].

[33] IBM Knowledge Center, «The Data Encryption Algorithm and the Data Encryption Standard,» [Ηλεκτρονικό]. Available: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.2.0/com.ibm.zos.v2r2.csfb300/csfb300_The_Data_Encryption_Algorithm_and_the_Data_Encryption_Standard.htm. [Πρόσβαση February 2017].

[34] Thomsen, S. S., & Knudsen, L. R. , «Technical University of Denmark - Cryptographic Hash Functions.,» 2009. [Ηλεκτρονικό]. Available: http://orbit.dtu.dk/files/5025771/sst_thesis_v1.0.pdf. [Πρόσβαση February 2017].

[35] FEDERAL INFORMATION PROCESSING STANDARDS, «Digital Signature Standard (DSS),» *Information Technology Laboratory,* 2009.

[36] RSA (cryptosystem), «Wikipedia - the free encyclopedia,» March 2017. [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/RSA_(cryptosystem). [Πρόσβαση March 2017].

[37] ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ, «Ασφάλεια Δικτύων,» 2001. [Ηλεκτρονικό]. Available: https://www.eap.gr/images/stories/pdf/PLI352_F31921.pdf. [Πρόσβαση 2017].

[38] CISCO, [Ηλεκτρονικό]. Available: http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html. [Πρόσβαση February 2017].

[39] Charlie Scott, Paul Wolfe and Mike Erwin, “Virtual Private Networks – Second Edition”, O’Reilly, 1999..

[40] P. Ravali, "A Comparative Evaluation of OSI and TCP/IP", International Journal of Science and Research (IJSR).

[41] Robert C. Raciti, «Using Frame Relay to Integrate the Enterprise,» 1996. [Ηλεκτρονικό].

[42] «Top Five VPN Advantages And Benefits,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[43] IP_Tunneling_and_VPN_Technologies, Cisco Systems, 2001.

[44] Mark Lewis, Comparing, Designing, and Deploying VPNs, Cisco Press, 2006.

[45] Μπούρας Ι. Χρήστος, «Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων,» Πανεπιστήμιο Πατρών, 2014. [Ηλεκτρονικό].

[46] Κωνσταντινίδης Χ. Αριστοτέλης, «Διαχείριση κινητικότητας και ασφάλειας σε ασύρματα Εικονικά Ιδιωτικά Δίκτυα,» 2004. [Ηλεκτρονικό].

[47] «Frame Relay vs X.25-Difference between frame relay and X.25,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[48] Jim Guichard, Ivan Pepelnjak, «Virtual Private Network Evolution,» Cisco Press, 2000. [Ηλεκτρονικό].

[49] Mark Lewis, «The ABCs of VPNs,» *PACKET,* 2006.

[50] «Understanding Virtual Private Networks,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[51] «VPN (Virtual Private Network),» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[52] «Το μοντέλο OSI,» [Ηλεκτρονικό]. [Πρόσβαση 2016].

[53] «Asynchronous Transfer Mode Switching,» sisco, 2016. [Ηλεκτρονικό].

[54] Charlie Scott, Paul Wolfe and Mike Erwin, Virtual Private Networks, United States of America: O'Reilly, 1999.

[55] M. Lewis, Comparing, Designing, and Deploying VPNs, Cisco Press, ISBN, 2006.

[56] MeetaGupta, Building a Virtual Private Network, Premier Press, 2003.

[57] R. Deal, The Complete Cisco VPN Configuration Guide, Cisco Press, 2005.

[58] A. G. Mason, CCSP self-study : Cisco Secure Virtual Private Networks (CSVPN)2nd Edition, Cisco Press, 2004.

[59] Ε. Κωλέτσου, «Επικοινωνίες και Δίκτυα Η/Υ,» pp. 5-6, 2010.

[60] Ε. Κωλέτσου, «Επικοινωνίες και Δίκτυα Η/Υ,» pp. 7-9, 2010.

[61] Μιχαήλ Λογοθέτης, «Τηλεπικοινωνιακά Δίκτυα Ευρείας Ζώνης,» [Ηλεκτρονικό].

[62] «MPLS FAQ For Beginnersl,» [Ηλεκτρονικό]. Available: http://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html.

[63] investintech, «PUBLIC AND PRIVATE KEY ENCRYPTION SYSTEMS,» [Ηλεκτρονικό]. Available: http://www.investintech.com/resources/articles/publicprivatekey/. [Πρόσβαση February 2017].

[64] Avi Kak, «Public-Key Cryptography and the RSA,» February 2016. [Ηλεκτρονικό]. Available: https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf. [Πρόσβαση February 2017].

[65] University of Technology, Sydney, «Internet Security Protocol (IPSec),» 48740 Communication

Networks, [Ηλεκτρονικό]. Available: http://services.eng.uts.edu.au/~kumbes/ra/Security/IPSec/IPSec.htm. [Πρόσβαση February 2017].

[66] Dave Kosiur, Building and Managing Virtual Private Networks, John Wiley & Sons, 1998.

[67] Mike Erwin, Charlie Scott, Paul Wolfe , Virtual Private Networks, O'Reilly Nutshell.

[68] DELL EMC, «RSA Laboratories,» [Ηλεκτρονικό]. Available: https://apj.emc.com/emc-plus/rsa-labs/standards-initiatives/s-wan.htm. [Πρόσβαση March 2017].

[69] Κώστας Λιμνιώτης, «Σχεδίαση Εικονικών Δικτύων - ΤΕΙ Λαμίας,» 2006. [Ηλεκτρονικό]. Available: http://cgi.di.uoa.gr/~klimn/vpn/VPN-lecture_notes.pdf. [Πρόσβαση 2017].

ΠΑΡΑΡΤΗΜΑ Α

Δίκτυο 1 – Configuration cisco router 2811.

```
HQ#show running-config
        Building configuration...

        Current configuration : 1244 bytes
        !
        version 12.4
        no service timestamps log datetime msec
        no service timestamps debug datetime msec
        no service password-encryption
        !
        hostname HQ
        !
        !
        !
        !
        !
        !
        !
        aaa new-model
        !
        aaa authentication login abc1 local
        !
        !
        !
        !
        aaa authorization network abc2 local
        !
        !
        !
        !
        !
        ip cef
        no ipv6 cef
        !
        !
        !
        username admin password 0 admin
        !
        !
        crypto isakmp policy 10
        encr 3des
        hash md5
        authentication pre-share
        group 2
        !
        !
```

```
!
crypto isakmp client configuration group cisco
key cisco123
pool VPNPOOL
!
!
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
crypto dynamic-map map1 10
set transform-set set1
reverse-route
!
crypto map map1 client authentication list abc1
crypto map map1 isakmp authorization list abc2
crypto map map1 client configuration address respond
crypto map map1 10 ipsec-isakmp dynamic map1
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.10.10.11 255.255.255.0
duplex auto
speed auto
crypto map map1
!
interface Vlan1
no ip address
shutdown
!
ip local pool VPNPOOL 192.168.1.1 192.168.1.50
ip classless
!
ip flow-export version 9
!
```

```
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
!
!
!
End
```

ΠΑΡΑΡΤΗΜΑ Β

Δίκτυο 2 – Configuration του SW1

```
SW1#sh running-config
Building configuration...

Current configuration : 2172 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0060.2F47.8741
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
```

```
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 10
```

```
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

Δίκτυο 2 – Configuration του SW2

```
SW2#sh running-config
Building configuration...

Current configuration : 2040 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW2
!
!
```

```
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 20
```

```
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
 switchport mode trunk
!
interface FastEthernet0/24
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
!
```

```
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

Δίκτυο 2 – Configuration του SW3

```
SW3#show running-config
Building configuration...

Current configuration : 2017 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW3
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 30
 switchport mode access
```

```
!
interface FastEthernet0/6
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 40
 switchport mode access
!
```

```
interface FastEthernet0/18
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

Δίκτυο 2 – Configuration του Switch 4

```
Switch#sh running-config
Building configuration...

Current configuration : 977 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
no service password-encryption
!
hostname Switch
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
```

```
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End
```

Cisco Router R1 Final Configuration:

```
R1#show running-config
Building configuration...

Current configuration : 3042 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 8
!
hostname R1
!
login block-for 120 attempts 5 within 45
!
!
enable secret 5 $1$mERr$2kSZR9DN2ofxLllbGij.S1
enable password 7 0832495E1D1C08151719
!
!
!
ip dhcp pool VLAN10
```

```
 network 172.16.10.0 255.255.255.0
 default-router 172.16.10.254
 dns-server 10.10.10.1
ip dhcp pool VLAN20
 network 172.16.11.0 255.255.255.192
 default-router 172.16.11.62
 dns-server 10.10.10.1
ip dhcp pool VLAN30
 network 172.16.11.64 255.255.255.224
 default-router 172.16.11.94
 dns-server 10.10.10.1
ip dhcp pool REMOTE_pool
 network 72.44.20.0 255.255.255.240
 default-router 72.44.20.14
 dns-server 10.10.10.1
!
!
aaa new-model
!
aaa authentication login REMOTE local
!
!
aaa authorization network REMOTE local
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username VPN secret 5 $1$mERr$RPINYfToCVNkXLYZxG/nv/
username bob secret 5 $1$mERr$oK3TI6nvyf.fqqapWfQpV/
username joe privilege 15 secret 5 $1$mERr$OIpuusDboF144ha1OqULI/
username olga password 7 0825494D0C14071200
username paul privilege 3 secret 5 $1$mERr$i.ZcPq2E1f0Zw0VoRpVH9.
!
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 2
 lifetime 21600
!
!
!
```

```
crypto isakmp client configuration group REMOTE
 key CISCO
 pool MYPOOL
!
!
crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac
!
crypto dynamic-map DYNMAP 10
 set transform-set MYSET
 reverse-route
!
crypto map CLIENT_MAP client authentication list REMOTE
crypto map CLIENT_MAP isakmp authorization list REMOTE
crypto map CLIENT_MAP client configuration address respond
crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNMAP
!
!
!
!
ip domain-name remotetrainingsolutions
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.16.10.254 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.11.62 255.255.255.192
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.11.94 255.255.255.224
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 172.16.11.110 255.255.255.240
```

```
!
interface FastEthernet0/1
 ip address 72.44.20.14 255.255.255.240
 duplex auto
 speed auto
 crypto map CLIENT_MAP
!
interface Serial0/0/0
 bandwidth 128
 ip address 88.40.12.1 255.255.255.252
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip local pool MYPOOL 172.16.10.150 172.16.10.200
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
!
banner motd ^C DO NOT ATTEMPT TO LOGIN AND ACCESS THIS ROUTER ^C
!
privilege exec level 3 show
privilege exec level 3 show startup-config
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 transport input ssh
!
!
```

```
!
end
R1#
```

Cisco Router 2 ISP Final Configuration:

```
ISP#show running-config
Building configuration...

Current configuration : 791 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ISP
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 10.10.10.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
```

```
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/0/1
bandwidth 128
ip address 88.40.12.2 255.255.255.252
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 172.16.10.0 255.255.254.0 88.40.12.1
!
ip flow-export version 9
!
!
!
no cdp run
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
ISP#
```